A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

The Journal of Public Inquiry

FALL/WINTER

2009-2010

COUNCIL OF INSPECTORS GENERAL ON
INTEGRITY AND EFFICIENCY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Journal of Public Inquiry. Fall/Winter 2009-2010	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Council of the Inspectors General on Integrity and Efficiency,1717 H Street NW Suite 825,Washington,DC,20006**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**60**	

Council of Inspectors General on Integrity and Efficiency

The *Inspector General Reform Act of 2008* created the Council of Inspectors General on Integrity and Efficiency. This statutory council supersedes the former President's Council on Integrity and Efficiency and Executive Council on Integrity and Efficiency, established under Executive Order 12805.

The CIGIE mission is to address integrity, economy, and effectiveness issues that transcend individual government agencies; and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

The CIGIE is led by Chair Phyllis K. Fong, Inspector General of the U.S. Department of Agriculture, and Vice Chair Carl Clinefelter, Inspector General of the Farm Credit Administration. The membership of the CIGIE includes 69 Inspectors General from the following federal agencies:

Members of the Council

Agency for International Development
Department of Agriculture
Amtrak
Appalachian Regional Commission
Architect of the Capitol
U.S. Capitol Police
Central Intelligence Agency
Department of Commerce
Commodity Futures Trading Commission
Consumer Product Safety Commission
Corporation for National and Community Service
Corporation for Public Broadcasting
The Denali Commission
Department of Defense
Office of the Director of National Intelligence
Department of Education
Election Assistance Commission
Department of Energy
Environmental Protection Agency
Equal Employment Opportunity Commission
Export-Import Bank of the United States
Farm Credit Administration
Federal Communications Commission
Federal Deposit Insurance Corporation
Federal Election Commission
Federal Housing Finance Board
Federal Labor Relations Authority
Federal Maritime Commission
Federal Reserve Board
Federal Trade Commission
General Services Administration
Government Accountability Office
Government Printing Office
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of Interior
U.S. International Trade Commission
Department of Justice
Department of Labor
Legal Services Corporation
Library of Congress
National Aeronautics and Space Administration
National Archives
National Credit Union Administration
National Endowment for the Arts
National Endowment for the Humanities
National Labor Relations Board
National Science Foundation
Nuclear Regulatory Commission
Office of Personnel Management
Peace Corps
Pension Benefit Guaranty Corporation
Postal Regulatory Commission
U.S. Postal Service
Railroad Retirement Board
Securities and Exchange Commission
Small Business Administration
Smithsonian Institution
Social Security Administration
Special Inspector General for Afghanistan Reconstruction
Special Inspector General for Iraq Reconstruction
Department of State
Tennessee Valley Authority
Department of Transportation
Department of Treasury
Treasury Inspector General for Tax Administration
Special Inspector General for the Troubled Asset Relief Program
Department of Veterans Affairs

LETTER FROM THE EDITOR-IN-CHIEF

The importance of the *Journal of Public Inquiry* can best be illustrated by the content provided in the Fall/Winter 2009-2010 edition, which highlights the critical role inspectors general play in the federal government from investigations to congressional testimony to prioritizing accountability. The *Journal* increases public awareness and ensures that government decision-makers, Congress, and the public are cognizant of the pivotal role inspectors general play in the economy, efficiency, and effectiveness of our respective agencies and departments.

This is a time of enormous challenge and responsibility for many of us who are working as "agents of positive change" in the federal government. We are in a different environment, one where new issues and technologies add complexity to the multitude of programs and operations we oversee.

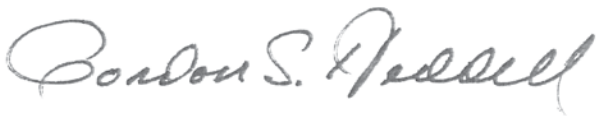
We do have challenges ahead, but this is also a time of great opportunities. We are committed in our mission to provide objective, independent, and professional oversight. However, the expectations from our respective agencies, Congress, and the public remain high. Statutory inspectors general are crucial to improving the efficiency of the executive branch through our expertise in audits, investigations, evaluations, and our knowledge of particular programs and operations.

And here lies the opportunity. The focus must turn to the generation of ideas and solutions. Partnerships must be cultivated and relied upon. We must come together in forums, such as the *Journal*, to delve into the heart of our mission and discover the changes we can make towards the advancement of our community.

The *Journal* includes six articles related to investigations, which address initiatives such as how to maximize recoveries in fraud cases and how to utilize a forensic document laboratory. One author shares his experiences in training foreign government officials unfamiliar with the IG concept, while another discusses the manner in which earlier inspectors general decisions likely influenced the perceptions of current IGs regarding their oversight responsibilities.

FBI Director Robert Mueller, and Inspectors General Daniel Levinson and Brian Miller address different audiences in speeches on cyber security, health care, and federal law enforcement. In addition, we include testimony of Inspector General Paul Martin on the challenges facing NASA and the testimonies of Inspector General Arnold Fields and Deputy Inspector General Kenneth Moorefield before the Commission on Wartime Contracting regarding challenges in Afghanistan.

So much of our future gives me pause for positive thought – not only in the difference we are making for our country, but in the ideas shared in this *Journal*. I encourage anyone with interest in the oversight community to read and lend support to the *Journal*. We are grateful to the editorial board and the authors for their significant contributions to our community.



Gordon S. Heddell
Inspector General

Journal of Public Inquiry

Council of the Inspectors General on Integrity and Efficiency

❧ Denotes the end of an article.

[INVESTIGATIONS]

Show me the Money! Maximizing Agency Recoveries in Fraud Cases

The coordination of all remedies - criminal, administrative, and contractual - is critical when investigating and resolving a fraud case

By Michael J. Davidson

Largely through the investigative efforts of the Office of Inspector General agents and other law enforcement entities, the XYZ Corporation and one or more of its employees is convicted and fined after defrauding the government. The miscreant corporate employees are incarcerated and the Department of Justice follows up with a civil False Claims Act lawsuit to extract additional penalties. Any relevant contracts will be terminated and a referral is made to the victim agency's Suspension and Debarment Official to debar the company and the defendant employees from future contracts. You close the case and move on to other things because there is nothing left to do, right? Wrong!

One important, and often overlooked aspect of a fraud case is facilitating the return of money back to the victim agency in order to make it whole. More often than not, the agency still needs the goods, services or funds that it lost through fraud. Fortunately, the law provides several mechanisms to make the victim agency whole, but many of these require advanced coordination and familiarization with the relevant legal authority. The early coordination of an agency recovery is not only important in terms of the practical necessity to include this in any plea or settlement negotiations, but also because of the legal time limits on the agency's ability to spend the money. Pursuant to 31 U.S.C. § 1553(a), all time limited appropriations cease to be available for obligation five years after its initial period of availability. After the five year period expires, the appropriations account is deemed closed and all unobligated funds must be returned to the Treasury's general fund. This article attempts to familiarize the OIG community with some of the legal avenues to return money, goods, and services to the victim agency.

THE MISCELLANEOUS RECEIPTS STATUTE

The primary legal obstacle for returning money to agency coffers is the miscellaneous receipts statute, which establishes the general rule that all money received by or for the United States must be returned to the Treasury Department. Specifically, the miscellaneous receipts statute, 31 U.S.C. § 3302(b), states that "an official or agent of the government receiving money for the government from any source shall deposit the money in the Treasury as soon as practicable without deduction for any charge or claim." The statutes mandate is a broad one. As one court noted, it applies to "money for the government *from any source* . . . . The original source of the money—whether from private parties or the government—is thus irrelevant."[1] The improper retention of funds not only would violate the miscellaneous receipts statute, but also would likely constitute an improper augmentation of an agency's appropriation.

However, like most laws, the miscellaneous receipts statute has exceptions, which may allow an agency to re-

1 Scheduled Airlines Traffic Office, Inc. v. Department of Defense, 87 F.3d 1356, 1362 (D.C. Cir. 1996) (emphasis in original).

tain monies received. The Government Accountability Office has opined that the statute does not apply when 1) an agency is specifically authorized by statute to retain money or 2) the money is a qualifying refund to the agency's appropriations.[2] GAO defined a refund "to include 'refunds of advances, collections for overpayments made, adjustments for previous amounts disbursed, or recoveries of erroneous disbursements from appropriation or fund accounts that are directly related to, and reductions of, previously recorded payments from the accounts.'"[3]

CRIMINAL RESTITUTION

Specific statutory authority exists that permits a victim agency to retain monies received in the form of criminal restitution. The Victim and Witness Protection Act of 1982, 18 U.S.C. § 3663, amended by the Mandatory Victim Restitution Act of 1996, 18 U.S.C. § 3663A, provides this authority. The Victim and Witness Protection Act authorizes a court to order a criminal defendant to make restitution to the victim of the crime. The Mandatory Victim Restitution Act made victim restitution mandatory for certain property crimes, crimes of violence, and consumer product tampering offenses. The definition of a "victim" is virtually identical for both statutes.

Significantly, a federal agency is considered a victim entitled to restitution. To illustrate, in *Refert v. United States*, 519 F.3d 752, 759 (8th Cir. 2008), the court, in a health care prosecution, upheld an order of restitution to the Indian Health Service, which is part of the Department of Health and Human Services, that covered the costs of emergency care services obtained through false representation. The court noted that "Government agencies that are victims of offenses involving fraud and deceit are entitled to restitution under 18 U.S.C. § 3663A(a)(1), the Mandatory Victim Restitution Act."[4]

However, there are some limitations on recovery. First, 18 U.S.C. § 3664(i) provides that when the United States is a victim, "the court shall ensure that all other victims receive full restitution before the United States receives any restitution." Further, in *Federal Motor Carrier Safety Administration,* B-308478 (Dec. 20, 2006), GAO discussed restitution in the context of the refund exception and limited agency retention of restitution to those amounts properly classified as a refund. In other words, the restitution must reflect an amount paid in error, overpaid or an adjustment of a previous amount dispersed. Unfortunately, GAO did not discuss the applicability or scope of the Acts.

CIVIL FALSE CLAIMS ACT

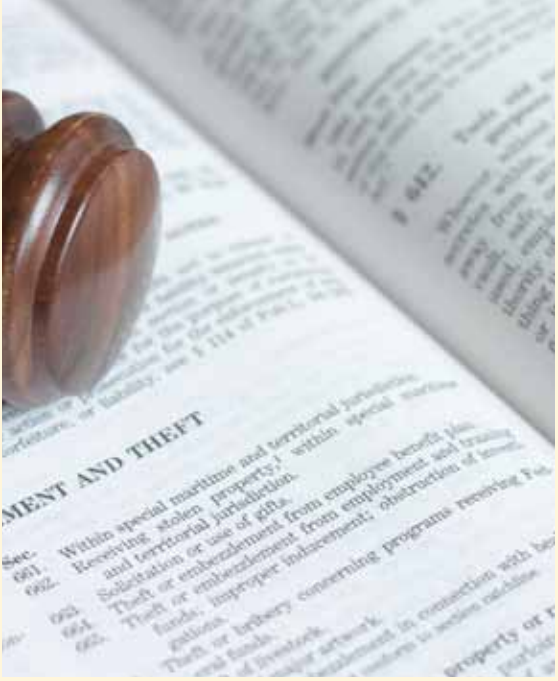
The civil False Claims Act, 31 U.S.C. §§ 3729-3733, is the government's primary weapon against fraud. The Act dates from the Civil War but was significantly strengthened in 1986 following the procurement scandals of the 1980s. Since 1986, DOJ has recovered more than $24 billion in False Claims Act settlements and judgments, including recovery of $2.4 billion in FY 2009 alone.[5] Significantly, for purposes of this article, section 3729(a) of the Act provides for the recovery of treble damages and penalties.

Although the False Claims Act does not specifically authorize a victim agency to retain any money recovered in a case, authority exists elsewhere for both the DOJ and a victim agency to retain a portion of a case recovery. First, DOJ retains three percent from the total

False Claims Act recovery.[6] The authority to retain this money derives from the statutorily created DOJ Three Percent Fund, whose originating legislation first appeared in 1993, but was repealed and reenacted in 2002 with more expansive parameters for DOJ's use of collected funds.[7] The fund is used to pay for various DOJ debt collection expenses and to support the U.S. Attorney Offices' Financial Litigation Units.

Second, GAO has opined that an agency may retain a portion of a recovery as a form of refund. Specifically, GAO has opined that "the refund exception . . . allows agencies to retain the portion of a settlement that represents amounts erroneously disbursed due to a false claim."[8] This exception permits an agency to retain that portion of the recovery that represents its "direct loss," or what is often referred to as "single damages" in the False Claims Act context.[9] However, GAO rejected an agency's request to retain treble damages and penalties. GAO applied to False Claims Act awards the general rule that penalties may not be retained by an agency, but instead must be deposited in the Treasury's

2 *Tennessee Valley Authority-False Claims Act Recoveries,* B-281064 (Feb 14, 2000), at 2; *Federal Emergency Management Agency-Disposition of Monetary Award Under False Claims Act,* B-230250 (Feb. 16, 1990), at 2.
3 FEMA, at 2.
4 519 F.3d at 759.
5 Press Release, Dep't of Justice, Justice Department Recovers $2.4 Billion in False Claims Cases in Fiscal Year 2009; More Than $24 Billion Since 1986, (Nov. 19, 2009).
6 *National Science Foundation-Disposition of False Claims Recoveries,* B-310725 (May 20, 2008), at n.3 ("DOJ deducts a 3-percent fee for its services from the total recovery").
7 See 28 U.S.C. § 527 note.
8 *NSF,* at 4.
9 *Id.; TVA,* at 3.



general fund as a miscellaneous receipt.[10] Additionally, GAO determined than any amounts exceeding an agency's actual losses must also be deposited as miscellaneous receipts.[11] In sum, a victim agency may only retain that portion of an award or settlement that represents the agency's actual losses that are directly related to the underlying misconduct.

INVESTIGATIVE COSTS

At least two earlier GAO decisions suggested that an agency could retain investigative costs as part of a False Claims Act award or settlement. First, in *Federal Emergency Management Agency-Disposition of Monetary Award Under False Claims Act,* B-230250 (Feb. 16, 1990), at 3, GAO permitted FEMA to deposit into the National Insurance Development Fund not only that portion of the False Claims Act award representing the amount erroneously paid out of the Fund because of false insurance claims, but also the amount of administrative expenses the Fund incurred investigating the insurance claims and preparing the case for trial. The National Insurance Development Fund was a revolving fund that received funding from several sources including insurance premiums and fees; and in turn served as the funding source for FEMA's federal crime insurance program.[12] Significantly, the Fund received no appropriations to pay for its administrative expenses or to reimburse it for any losses. [13]

Second, in *Tennessee Valley Authority-False Claims Act Recoveries,* the agency was permitted to retain, by depositing in the TVA Fund, not only "moneys erroneously disbursed on the basis of the false claim," but also "investigative costs . . . directly related to the false claim."[14] The Tennessee Valley Authority was a wholly owned government corporation financed by the sale of power, the revenue from which was deposited into the TVA Fund. GAO determined that the refund exception applied to "investigative costs that are directly related to the false claim. These are a direct consequence of the false claim paid, and increased TVA's losses."[15]

However, in two clarifying opinions, GAO severely limited an agency's authority to recover investigative costs when the agency received an appropriation for the conduct of investigations. In the *Federal Motor Carrier Safety Administration* opinion discussed above, GAO restricted agency retention of investigative costs in the form of criminal restitution to amounts meeting the definition of a refund. Next, in *National Science Foundation – Disposition of False Claims Recoveries,* B-310725 (May 20, 2008), GAO rejected a request from the National Science Foundation Inspector General to credit to the IG's appropriations that amount of a False Claims Act recovery representing the IG's investigative costs. GAO reasoned that recovery of the IG's investigative costs did not qualify as a refund because they were "not payments made in error, overpayments, or otherwise adjustments to amounts previously disbursed," rather such costs "are payments properly made from an appropriation that is available for incurring costs for such investigations."[16] The fact that the agency received appropriated funds to conduct investigations distinguished these opinions from the *TVA* and *FEMA* opinions.

GOODS AND SERVICES

One point that becomes particularly important when negotiating a settlement with a criminal defendant or civil False Claims Act defendant is that the miscellaneous receipts statute only applies to the receipt of money and not to the receipt of goods or services.[17] Accordingly, the miscellaneous receipts statute restrictions are not triggered when an agency receives goods or services, rather than money, as part of a settlement agreement. Further, the receipt of such goods or services does not require an "offsetting transfer from current appropriations to miscellaneous receipts" and the miscellaneous receipts statute remains inapplicable even if the agency could have received money, rather than goods or services, and such money would have been otherwise returned to the Treasury.[18] It may be easier for a defendant to settle a case by providing replacement goods and services rather than by paying a monetary settlement. Indeed, it is not uncommon for DOJ to settle False Claims Act cases and require the provision of goods or services to the victim agency as part of the settlement agreement.[19] Further, 18 U.S.C. § 3664(f)(3)&(4) specifically authorizes restitution in the form of property replacement or services.[20]

10 *FEMA,* at 4.
11 *Id.*

12 *Id.* at 1.
13 *Id.* at 3.
14 *TVA,* at 3.
15 *Id.* at 3.

16 *NSF,* at 4.
17 *Bureau of Alcohol, Tobacco, and Firearms—Augmentation of Appropriations—Replacement of Autos by Negligent Third Parties,* B-226004 (July 12, 1988).
18 *Id.; see also* Procurement Fraud Division (PFD) Note, *The Miscellaneous Receipts Statute and Permissible Agency Recoveries of Monies,* Army Lawyer (March 2001), at 36.
19 PFD Note, *supra,* at 35 (DoJ settlement agreement with a defense contractor that included millions of dollars worth of goods and services).
20 Bureau of Prisons-Disposition of Funds Paid in Settlement of Breach of Contract Action,

CONTRACT RELATED RECOVERIES

An agency may recover, and retain, money through various contractual mechanisms. A principal vehicle for recovery includes reprocurement costs associated with contracts tainted by fraud. For example, in *Appropriation Accounting-Refunds and Uncollectibles,* B-257905 (Dec. 26, 1995), GAO posited that money recovered under a fraudulent contract, in this case from an embezzler, qualified as a refund that the agency could deposit "to the credit of the allotment/appropriation against which the payments previously were charged . . . ." Similarly, in the event of a contract breach, including fraud-based terminations for default, the agency may retain any funds received as a remedy for the default and use them to fund a replacement contract, including money that exceeds the cost of the original contract, so long as the excess money serves to make the agency whole and the agency procures similar goods or services.

FORFEITURE FUNDS

Finally, an agency may seek the recovery of money through forfeiture funds. At least two such funds contemplate payment of forfeited funds to federal agency victims - the DOJ Asset Forfeiture Fund and the Treasury Forfeiture Fund. Title 18 United States Code Section 981(e)(6) authorizes the Attorney General, the Secretary of the Treasury, and the Postal Service to transfer forfeited property as restoration to victims of an offense. A victim is defined as a person, including a legal entity, "who has incurred a pecuniary loss as a direct result of the commission of the offense underlying a forfeiture." 28 C.F R. § 9.2(m),(v).

In cases of judicial forfeiture, the victim agency can submit a petition for remission of forfeited assets to the Assistant U.S. Attorney handling the case, who in turn will forward the petition, with recommendations concerning the petition from the United States Attorney's Office and the seizing agency, to DOJ's Asset Forfeiture and Money Laundering Section. 28 CFR §§ 9.1(b)(2); 9.4(f). This generally will decide the petition after all relevant assets have been forfeited and a final order of forfeiture is received.

CONCLUSION

The coordination of all remedies – criminal, civil, administrative, and contractual – is critical when investigating and successfully resolving a fraud case involving the United States. One such remedy is the recovery of funds to the victim agency lost to fraud so that the agency can obtain the goods and services that it still needs, and that Congress originally intended it receive. As described in this article, several legal avenues exist to recover those funds, but the procedures are often complex and require advanced planning and coordination. ❧

B-210160 (Sept. 28, 1983).

Michael J. Davidson

Michael J. Davidson is a supervisory contract and fiscal law attorney with the Office of the Principal Legal Advisor, Immigration and Customs Enforcement. He has previously served as a litigation and supervisory attorney with the Department of the Treasury. He also practiced law as an Army judge advocate, retiring from the Army after 21 years of service.

His prior assignments have included branch chief with the Army Procurement Fraud Division, as special assistant U.S. attorney in Arizona specializing in procurement fraud and public integrity prosecutions, and as a special trial attorney with DOJ's civil fraud section.

Mr. Davidson earned his Bachelor of Science degree from the U.S. Military Academy, his J.D. from the College of William & Mary, a LL.M. in Military Law from the Army's Judge Advocate General's School, a second LL.M. in Government Procurement Law from George Washington University, and a Doctor of Juridical Science in Government Procurement Law from GWU. His doctoral dissertation focused on procurement fraud.

[INVESTIGATIONS]

A Special Expertise: Forensic Document Laboratory

Much like a fingerprint, an individual's handwriting is unique, and therefore identifiable to a single person

By Nancy Cox and Kirsten Singer

The Veterans Affairs Office of Inspector General is tasked with perhaps one of the most honorable of all IG missions: to protect and provide care, support and recognition for America's veterans and their families. The VA OIG fulfills this mandate through five primary Offices: Investigations, Audit, Healthcare Inspections, Contract Review, and Management and Administration. Each of these offices provides critical services to veterans and each has access to a highly specialized unit that frequently provides convincing resolution in investigations -- the VA OIG Forensic Document Laboratory.

Established within the Veterans Administration in the 1950s, the Forensic Document Laboratory was originally known as the "Identification and Detection Laboratory" of the Investigation Service, Office of Appraisal and Security, Washington, D.C. Then, as today, a majority of the laboratory's casework involved disputed documents submitted by VA claimants. When the VA OIG was created in 1978, the laboratory was incorporated into its mission capabilities, and continues to provide invaluable assistance in criminal and administrative investigations. Today's laboratory serves 128 VA OIG criminal investigators nationwide and conducts approximately 100 examinations a year involving thousands of documents. The laboratory is equipped with state-of-the-art forensic document instrumentation and conducts all aspects of traditional document examination.

Forensic Document Expertise

Forensic document examination – also known as "questioned documents" or "handwriting analysis" – is one of the oldest of the forensic sciences. In 1910, the forensic document profession garnered official status in the United States with the publication of the book "Questioned Documents" by Albert S. Osborn, an examiner who later identified Bruno Hauptmann's writing in ransom notes to Charles Lindbergh in the "trial of the century." Over time, the examination of questioned documents came to be recognized as a skill that required specialized training to achieve competency.

The term "questioned document" usually refers to any kind of paper that contains handwritten or machine markings whose authenticity or origin is at issue. Questioned writings, however, may also be found on such "documents" as walls, boxes, doors, and even on victims of homicide. Known primarily as a discipline that examines and compares questioned and known writings to determine authorship, this expertise also

encompasses a myriad of other kinds of document examinations, including authenticating and dating documents; deciphering indented, erased, obliterated, charred and water-soaked documents; examining and comparing typewritten entries; and conducting paper and ink analyses. The explosion of technology in the latter half of the twentieth century expanded the role of the document examiner to include the examination of documents generated using such machines as photocopiers, faxes, and computer printers.

By far, the most frequently requested forensic document examination is the comparison of questioned writing with the known writing of a subject to determine whether or not the subject produced the questioned writing. Much like a fingerprint, an individual's handwriting is unique, and therefore identifiable to a single person. Unlike a fingerprint, however, handwriting can not only change over time, it is also susceptible to other influences, such as disguise, illness, medications, and writing surface. These variables, combined with the twenty-first century's predilection to replace original documents with copies, resulted in the need for examination conclusions that express the extent of a document examiner's certainty based on the evidence at hand. These conclusions range from identification to elimination, with degrees of certainty in between. This conclusion terminology has been standardized and published by the American Society for Testing and Materials, and is referred to as Standard Guide E1658, Standard Terminology for Expressing Conclusions of Forensic Document Examiners. The Forensic Document Laboratory adheres to this standard, as well as 17 other published forensic document examination standards -- the greatest number of ASTM standards published by any forensic discipline to date.

How does one become a forensic document examiner? There are a variety of undergraduate and graduate degree programs that offer forensic document examination courses, and these provide a good general foundation for this forensic science. But the true expertise is acquired through an apprenticeship program, lasting at least two years, under the purview of qualified, experienced forensic document examiners. Literally thousands of handwriting samples must be examined over time before an examiner develops the expert ability to discriminate individual handwriting features from those that are more common. The training period also includes the many other aforementioned document examinations, as well as report writing, testimony preparations, and moot courts. Following this rigorous training period, a fully-trained forensic document examiner is then eligible to apply for national certification through the American Board of Forensic Document Examiners. The Board was established in 1977 with a grant from the Department of Justice to provide, in the interest of the public and the advancement of science, a program to recognize qualified forensic document examiners in government and private laboratories. The Board certification process requires a credentials review, after which the candidate must successfully pass comprehensive written, practical, and oral examinations. The laboratory currently has two Board certified forensic document examiners with a combined experience of more than 35 years. Both examiners are active in regional and national forensic science organizations, and one of the examiners is a national subject matter expert in *Daubert* legal admissibility challenges. *Daubert* refers to a 1993 Supreme Court decision in which judges were assigned the responsibility of being the "gatekeepers" for allowing expert testimony at trial. By applying criteria such as whether an expertise is generally accepted, has an established error rate, and complies with standard procedures, the judge can presumably determine the reliability of an expertise and admit it for trial. The forensic sciences continue to be challenged by *Daubert,* but forensic document examination has become the model for addressing *Daubert* challenges in the forensic community.

The forensic document examiners of the VA OIG conduct each examination independently and objectively, issuing a written report at the completion of an examination and testifying to their findings in court when called to do so. To further ensure quality and accuracy, independent technical and administrative reviews are conducted by a second Forensic Document Laboratory examiner for every document case.

VA Document Cases

The role of forensic document examination in the criminal justice process is significant. A qualified examiner may be asked to resolve many issues concerning the origin or validity of a document in nearly every type of crime. While investigations of the VA OIG are diverse ranging from procurement fraud, bribery, embezzlement, and identity theft, to patient abuse, sexual assault and homicide, a common denominator in each case is the documents. Disputed or incriminating documents are often critical evidence in a multitude of offenses.

Over the last three years, approximately 85 percent of the cases submitted to the laboratory have been examined in order to determine authorship of a questioned document while the remaining 15 percent involved other aspects of documents including alterations and indentations. A conclusion regarding a document's authenticity (e.g., genuine date/time period) was reached in 90 percent of the cases. More than half of the disputed handwriting cases examined by the laboratory substantiated some level of fraud. These forensic document

examinations have contributed not only to numerous convictions and reimbursements, but also avoidance of unnecessary or unwarranted costs. Most importantly, these examinations have enabled the proper disbursement of benefits to veterans and their families.

Stolen Valor

Unequivocally, cases that receive the highest priority are those that imperil life or liberty. However, the VA OIG recognizes another category that is nearly equal in gravity – the false claim, manufacture, or sale of any military decoration, medal, badge or other award. Known as Stolen Valor, this offense became a federal crime for all military awards through the Stolen Valor Act of 2005. Each military award has an associated monetary compensation, so "adding" awards to a military record can increase a veteran's compensation. The document most often exploited in this pursuit is the Department of Defense Form DD-214, Certificate of Release or Discharge From Active Duty. This form is completed at the time of discharge from the military, and chronicles a veteran's years in service, as well as the various military awards that have been earned throughout a career.

The Forensic Document Laboratory frequently has a critical role in determining whether an original DD-214 has been altered, or even counterfeited. Detection of such fraud obviates monetary loss to VA, but more importantly, it protects the value of these revered emblems of courage. In a recent Stolen Valor investigation, a veteran altered his DD-214 as well as other military records. The veteran claimed to have been wounded in combat and to have earned several medals of valor, including the Purple Heart and Silver Star. As a result, the veteran used his fraudulent military history to bolster his credibility and receive unearned increased VA benefits. The veteran was prosecuted and sentenced to 366 days incarceration, 3 years probation, and ordered to pay restitution. The loss to VA was over $95,000 dollars.

In another case involving an altered DD-214, an honorably discharged veteran attempted to expand his list of medals from two to seven, including an unearned Purple Heart medal and a Combat Infantry badge (ironically, one of his two genuine awards was a Good Conduct Medal). In this case, the forensic document examiner determined that the questioned DD-214 and an original file copy originated from the same source document, with some notable discrepancies. The additional typewritten awards on the wayward document were not only out of vertical and horizontal alignment with the original typewritten entries, they were also typed using two different font styles (Figures 1 and 2).

Figure 1. An example of an altered DD214. "SILVER STAR" was added to the form and is not in vertical alignment with the other original entries.

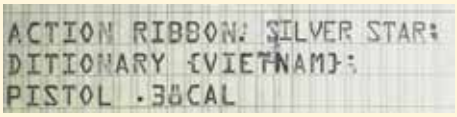
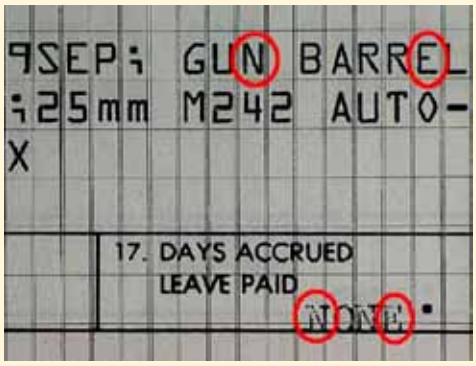


Figure 2. Two different type fonts were used in the alteration of the DD214. Examples of the different font styles are highlighted in red.



Handwriting Comparisons

The majority of the forensic examinations conducted by the VA OIG Forensic Document Laboratory involve the comparison of questioned and known writings (Figure 3).

In a not-so-recent case, but one that is distinct for its bravado, a veteran's wife provided a letter to VA that she claimed to have received from President John F. Kennedy in November 1960. In the letter, the President assures the wife that not only is he "fully aware of her husband's condition and needs," but that his claim for benefits compensation would be investigated by "the proper legal authorities." The letter itself is typed, but contains a signature in the name John Kennedy. Perhaps the wife believed that by invoking the President's name and personal interest in her case that no one would question the legitimacy of the letter. Nevertheless, it was swiftly determined that the signature in question was a poorly executed forgery of a genuine Kennedy signature.

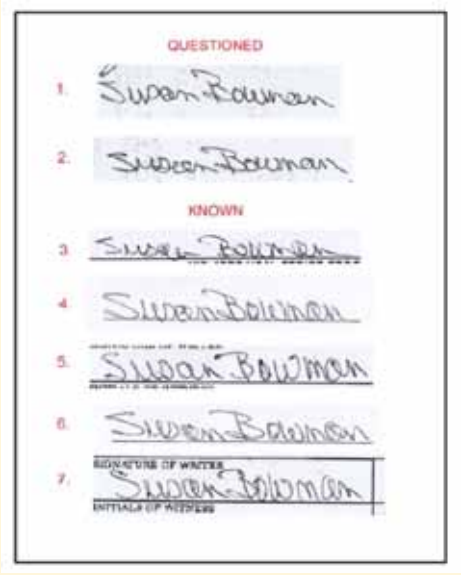
Today's criminal investigations involve much the same type of deception. In a recent criminal investigation, a former associate director of a Consolidated Mail Outpatient Pharmacy, his wife, and her staffing company were charged with conspiracy to commit wire fraud. The associate director had created the staffing company in 2000 to provide temporary pharmacists, at a higher pay rate, to the Outpatient Pharmacy. He then sought Small Business Administration certification as a woman-owned, minority-owned small disadvantaged business and 8(a) Program participant, then falsely claimed that the company was solely managed by his wife. The VA OIG Forensic Document Laboratory determined that the director had not only fraudulently signed his wife's name on the business' originating documents, but he continued to do so on the daily transactions. The associate director was also charged with wire fraud for making materially false misrepresentations to VA and other government officials. Between 2000 and 2007, the defendants and other unindicted co-conspirators used the

company to bill the VA for more than $8 million in services.

VA administers a number of financial benefit programs for eligible veterans and their family members. Among the benefits that are VA guaranteed home loans, education, insurance, and other monetary benefits. When those eligible to receive such benefits pass away, the temptation for others to continue receipt of the benefits occasionally results in the lack of notification to VA of the recipient's death. To detect such lapses, the VA OIG conducts an ongoing "death match" project that identifies deceased beneficiaries. In one of many "death match" cases, the Forensic Document Laboratory compared the questioned endorsements on 22 beneficiary checks with the writing of the deceased beneficiary's son, and determined that the beneficiary's son had written all of the questioned endorsements. He was sentenced to 3 years' probation and ordered to pay $21,529 in restitution to VA. In another case, the VA OIG received information that a deceased veteran had continued to receive VA pension benefits for six years after his death in 2000. Records revealed that over $122,000 had been electronically deposited after his death. VA was able to reclaim over $57,000 from the existing account, and when the laboratory concluded that it was highly probable that a family member had been endorsing the purloined checks, a guilty plea resulted. Sentencing consisted of 48 months probation, and over $65,000 in restitution.

The Forensic Document Laboratory also frequently provides assistance in administrative cases in areas of VA that are outside of the OIG, in particular the VA's Regional Office Insurance Center. The majority of the cases from the center involve contested insurance beneficiary forms. Before the center will disperse payment on a contested beneficiary form, the document in question is submitted to the laboratory to determine whether the veteran actually did sign his or her name. In 60 percent of the cases, the evidence indicates forgery.

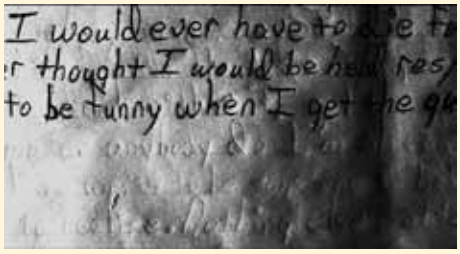
Figure 3. When conducting a handwriting examination, the questioned writing is compared to the known writing of an individual. The Forensic Document Laboratory constructs charts like the one below as demonstrative evidence for each conclusion.



Indented Writing

Sometimes the document evidence is not immediately visible. "Indented writing" refers to the writing impressions left behind, usually on paper beneath the writing surface (Figure 4). In an investigation involving the impersonation of a physician, documents were sent to the Forensic Document Laboratory for indented writing analysis. The forensic document examiner developed and deciphered indented writing on a pad of paper obtained from the individual's residence. The indented writing included names and phone numbers of various nurses and hospitals. The OIG investigation determined that an applicant at the VA Medical Center was fraudulently presenting himself as a military officer and surgeon with extensive education and professional experience. The defendant was sentenced to 12 months and one day of incarceration, three years' probation, and ordered to pay restitution of $42,758 to two female victims after pleading guilty to making a false statement and wire fraud.

Figure 4. Indentations can be deciphered from previously written entries.



Dating Documents

From 1901 through World War II, a group of Filipino soldiers in the Philippines – known as the Regular Philippine Scouts – were recognized as an integral extension of the U.S. Army in the Pacific. Considered "the backbone" of the American defense against Japan during WWII, veterans of the Regular Philippines Scouts who served with U.S. forces before October 6, 1945, are entitled to the same VA benefits as any veteran of the U.S. military. In an effort to receive, or increase, VA compensation, some Filipino citizens will submit medical or military documents as evidence that such compensation is due. When there is a question of authenticity, the VA's Regional Office Insurance Center in the Philippines submits the questioned documents to the laboratory to determine whether these documents were truly produced in their purported time period, usually the 1940s. In a recent case, the overwhelming smell of coffee wafted out as the questioned document was removed from its packaging. Coffee, tea, milk and vinegar are liquids commonly used to artificially age paper (Figure 5). The questioned document in this case was a Commonwealth of the Philippines, Philippine Army Enlistment

Record, allegedly typed on February 28, 1946. Under magnification, however, the entire text of the document, including the "signature," was found to have been produced using an inkjet printing process, which was not available until the mid-1970s.

Figure 5. When documents age naturally, discoloration is expected to be consistent throughout the document (below). Conversely, when a document is artificially aged, the results are sporadic and inconsistent areas of discoloration (bottom).

Research

The VA has one of the largest repositories of personnel files containing original documents dating back for decades. Recognizing the abundance of potential for research, the laboratory is currently conducting various research projects, such as the evolution of a person's signature over time, whether indented writings are still present on documents that are over twenty years old, and what impact medical ailments have on handwriting. This research may provide insight into examinations supporting criminal investigations with added benefit to the forensic document profession. The laboratory is also developing a virtual library of historical versions of the DD-214 for reference in Stolen Valor cases involving alterations and wholesale counterfeiting of this document.

Assisting Other OIGs

Because the Inspector General community shares many of the same criminal and administrative issues, and the VA OIG is one of only a few IGs with direct access to forensic document examination, the laboratory provides forensic examinations to any of the other 68 statutory IG offices on a case-by-case basis. Recently, the laboratory completed examinations for the Federal Trade Commission, Small Business Administration, and Health and Human Services IG offices.

Conclusion

The Office of Inspector General is dedicated to helping the Department of Veterans Affairs to serve America's veterans and their families. Integral to the VA OIG's success is its highly-skilled and well-trained Forensic Document Laboratory. Together, they ensure that the core values of integrity, economy and effectiveness are not only maintained, but thriving as they impact veterans, Veterans Affairs and the nation. ❧

Nancy Cox

Nancy Cox is the director of the Forensic Document Laboratory for the Department of Veterans Affairs Office of Inspector General. Ms. Cox oversees the centralized Laboratory which provides support for all of the Office of Inspector General. She has been a forensic document examiner for twelve years. She began her career with the U.S. Secret Service before coming to the VA OIG Forensic Document Laboratory in May 2006. Mrs. Cox is certified by the U.S. Secret Service as well as the American Board of Forensic Document Examiners and is a member of the Mid-Atlantic Association of Forensic Scientists. Mrs. Cox received her bachelor's degree from the University of Maryland.

Kirsten Singer

Kirsten Singer has been a forensic document examiner for 23 years. She began her career with the Virginia Division of Forensic, followed by the Treasury Inspector General for Tax Administration and U.S. Postal Inspection Service forensic laboratories before coming to the VA OIG Forensic Document Laboratory in April 2009. Ms. Singer is certified by the American Board of Forensic Document Examiners, where she served on the board of directors for five years, and is a member of the American Academy of Forensic Sciences and the American Society for Testing and Materials. Ms. Singer received her bachelor's degree from the University of Virginia and holds a Master of Forensic Science degree from the George Washington University.

[INVESTIGATIONS]

Model Protocol for Search Strings in Public Corruption Cases

The protocol was developed based on the fact that fraudsters use common hiding places and methods to make illicit payments

By Colin May

Corruption, bribes and kickbacks are among the most corrosive problems democracies face. They erode public trust in the government and degrade the rule of law. Individuals that corrupt elected and appointed government officials with cash, gifts, and rewards, must be investigated and prosecuted.

This article proposes a methodology for examining computers and digital evidence, specifically e-mail communications, for evidence of public corruption. In using this protocol, corruption investigations will be more productive, efficient, and allow for investigators and prosecutors to better identify cases suitable for prosecution.

Corruption Basics

An introduction to corruption is necessary in order to better assist the reader in the concepts presented here. Corruption is defined by the legal scholar and historian John Noonan as "an inducement, improperly influencing the performance of a public function."[1] According to the Association of Certified Fraud Examiners *Report to the Nation 2008*, corruption accounts for nearly 30 percent of the reported occupational fraud.[2] The median loss to corruption schemes is $375,000 – almost $240,000 more than its nearest rival: check tampering.

Corruption is a silent conspiracy where a government employee, elected official or appointed officer, enters into an illicit compact to enrich another party and themselves. Prevalent in the infamous Tammany Hall political organization in New York City, corrupt officials violate the public trust. These officials care more about themselves, their elections, and their benefactors than the greater good of the community. For example, convicted felon and former Congressman Randall "Duke" Cunningham (R-CA) created a "bribe menu," specifying that for every x-dollar contract, he expected y-dollars in gifts, gratuities, and cash. Cunningham, the now disgraced naval aviator, pleaded guilty.[3]

Most states have bribery, conspiracy, and financial disclosure statutes in place for public servants. Bribes, as defined by federal law (Title 18 United States Code, Section 201) are essentially monetary rewards, promises, or value-bearing items that are given to a public official in exchange for influencing an official act or improperly influencing the official. Bribes are different from extortion, where the "bribe-giver" is forced to give something of value to the bribe-taker, who is usually a public official. In addition to extortion statutes, mail and wire fraud laws, and false statements

1 Noonan Jr., John T. *Bribes*. Macmillian: New York, 1984, p. xi

2 ACFE, Report to the Nation 2008, p. 14, available at http://www.acfe.com/resources/publications.asp?copy=rttn

3 United States v. Randall Harold "Duke" Cunningham. Indictment, dated November 28, 2005 http://news.findlaw.com/wp/docs/crim/uscnnghm112805cinf.pdf and San Diego Union Tribune. "Randy 'Duke' Cunningham Case." http://www.signonsandiego.com/news/politics/cunningham/

are used by prosecutors as the primary means of acting against corrupt public officials. [4]

The ACFE further refines corruption fraud schemes into three major categories: bribery, gratuities, and conflicts of interest. Bribery, as described above, is conducted through two primary vehicles: contract bid rigging and invoice kickbacks.[5] Bid riggings are "contracts [that] are rigged, or manipulated, for criminal purposes…to obtain the contract award [and]…defrauding the victim," the government.[6] Kickbacks are portions of money that are given back to the corrupt official as remuneration. Gratuities are essentially gifts given for "consideration" of past or future official acts. The U.S. Supreme Court stated the difference best: "bribery requires intent 'to influence' an official act or 'to be influenced' in an official act, while illegal gratuity requires only that the gratuity be given or accepted 'for or because of' an official act."[7]

Conflicts of interest are schemes that violate "the legal principle that a fiduciary, agent, or employee must act in good faith, with full disclosure, and in the best interest of the principal or employer."[8] An analysis of the criminal prosecutions reported by the Office of Government Ethics shows that the most common criminal prosecution by the federal government is for violation of 18 USC 208, "Official Actions Affecting Personal Financial Interests."[9] This mirrors the ACFE results that show that private organizations are also similarly defined: "in order to be classified as a conflict of interest scheme, the employee's interest in the transactions must be undisclosed. The crux of a conflict of interest case is that the fraudster takes advantage of his employer; the victim organization is unaware that its employee has divided loyalties."[10]

Some examples of conflict of interest violations from the Office of Government Ethics' Prosecution Survey include:

- Lester Crawford, the head of the Food and Drug Administration, owned stock with his wife in "significantly regulated" companies that the FDA had primary oversight authority over. He failed to both report the stock ownership and recuse himself from any dealings with, or decisions about, the companies. In fact, Crawford "participated personally and substantially" in meetings that discussed issues related to the two companies in which he owned stock.
- A senior executive/branch chief at the National Institutes of Mental Health was approached by Pzifer Pharmaceuticals to collaborate with the senior executive and his branch on Alzheimer's disease research. Pfizer then paid him a significant retaining fee and travel expenses that totaled over $250,000. He did this without disclosing it, as required.
- The General Services Administration's director of property management in Kentucky was living with a GSA contractor, with whom she had oversight of the contracts. Her children also worked intermittently for the company while she made GSA contracting decisions without disclosing their relationship.

COMPUTERS, E-MAIL, AND CORRUPTION

No one can argue that computers and information technology has changed the landscape of our global commerce platform, nor of the American culture. Whether it's been made better or worse is for the philosophy and sociology majors to debate. But the change in our daily lives is not minor—and as we adapt these technologies, so do criminals. Law enforcement across the country investigate identity theft, criminal fraud, and computer misuse on a daily basis, and the epidemic of crimes involving digital technology and computers has just begun.

Making Illicit Payments & Transfers

- √ Corrupt gifts and favors
- √ Cash payments
- √ Checks & other instruments
- √ Hidden interests
- √ Fictitious loans
- √ Transfers at other than fair market value
- √ Future promises
- √ Floating
- √ Lapping
- √ Cooking

The complex nature and sophistication of hiding tools, coupled with the fragile nature of digital evidence, make the examination of computers for evidence of criminal activity very important. Criminals use the Internet and/or e-mail to trade, share, conceal, distribute, communicate, and coordinate information, documents, files, and other media.[11] Strader warns that "as commercial transactions increasingly become electronically-based, most types of white collar crime will involve computers to some extent," including corruption cases.[12]

4 Strader, J. Kelly. Understanding White Collar Crime. Second edition. LexisNexis: Newark, NJ 2006, p.169-170

5 Association of Certified Fraud Examiners. Fraud Examiners Manual. (2006 Austin, TX) FEM 1.701-1.738

6 Silverstone, Howard and Howard R. Davia. Fraud 101: Techniques and Strategies for Detection. Second edition, Wiley: New York, 2005, p.113

7 *Supra* note 3, at 173

8 *Supra* note 4, at 1.730

9 United States Office of Government Ethics. "Conflict of Interest Prosecution Survey Index" http://www.usoge.gov/laws_regs/other_ethics_guidance/othr_gdnc/pros_srvy_indx_st.html#Anchor-18664, retrieved 18 February 2010

10 *Supra* note 3, at 173

11 National Institutes of Justice. "Investigations Involving the Internet and Computer Networks." NCJRS, 2007 (NCJ 210798) www.ncjrs.org, p.1

12 *Supra* note 3, at 173

One prominent example of e-mail being used as evidence involved Darleen Druyun. Because of her position with the Air Force and her contract authority over Boeing, Druyun was able to secure positions at the defense plant for her daughter and son-in-law. E-mails exchanged between Druyun's daughter (possibly acting as Druyun's surrogate) and Boeing's chief financial officer negotiated her post-government employment with Boeing. One e-mail includes the chief financial officer stating "... had a 'non-meeting' yesterday re: hiring [Druyun]... Good reception to job, location, salary, longer-term outlook. Recommend we put together formal offer..." In her post-conviction debriefings with prosecutors, Druyun admitted making favorable decisions for Boeing, to ingratiate herself with the senior management of the company. She was eventually convicted of criminal conflict of interest charges, as was Boeing's CFO.[13]

The Druyun case highlights the use of e-mail evidence in conspiracies involving public corruption. This paper postulates a module to use when conducting digital forensic examinations of computers and e-mails, specifically. National Institute of Justice believes that "e-mails can be a starting point or key element in many investigations. [It] is the electronic equivalent of a letter, or a memo, and may include attachments or enclosures."[14] Investigators seeking further information on the role of electronic mail should consult the National District Attorney's Association guides on e-mail available from www.ndaa.org.[15]

13 May, Colin. "Lessons Learned from Acquisition Fraudster Darleen Druyun." Fraud Magazine (ACFE, Austin). May/June 2006. http://www.acfe.com/resources/view-content.asp?ArticleID=577

14 *Supra* note 10, at 1

15 NDAA, "Understanding E-mail: A Primer for Local Prosecutors" from http://www.ndaa.org/pdf/understanding_email.pdf; also see "The ECPA, IPSs, and Obtaining E-mail" from http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf. Retrieved 18 February 2010

MODEL PROTOCOL

When conducting an examination of computers, a "search string" method is used. Search string is defined as "a sequence of characters, words, or other elements that are connected to each other in some way. [It] usually refers to a string of words or a phrase that is used to search and locate or retrieve a specific piece of information contained in a database or set of documents."[16] Strings are vital to investigations and can uncover evidence needed to prosecute public corruption. Because of the hidden nature of corruption, e-mails can uncover evidence of illicit payments and asset transfers.

The protocol was developed based on the fact that fraudsters use common hiding places and methods to make illicit payments and transfers to conceal, disguise, and retrieve the profits of their crimes. It is assumed that two conspirators will communicate via electronic mail at some point in their relationship regarding several categories of activities, behaviors, and intentions regarding their criminality. These can fall into one or more of the following seven sets:

1. Prima facia evidence
2. Improper business relationship
3. Specific issue/case identities
4. Cash exchange
5. Asset transfer, concealment, or disguise
6. Investigation or audit
7. Cover-up and tampering

Searching based on the strings will enable a more organized, efficient, and productive examination of the suspect's computer and e-mail account. One note of caution should be amplified: one or two isolated positive search results are not indicative of corruption or fraud,

16 Search String" definition from www.learnthenet.com/english/glossary/string.htm; retrieved 18 February 2010

Sample Search Strings by Category (Public Corruption)

Prima Facia Evidence
- Bribe
- Illegal bribe
- Gratuity
- Illegal gratuity
- Graft
- Kickback
- Special gift

Improper Business Relationship
- Job
- Title
- Contract
- Sweetheart contract
- Duties
- Spot
- Wife's job
- No-show job
- Noshow job
- No show job

Cash Exchange
- Hush money
- Favor
- Favors
- Money
- Cash
- Fee

Asset Transfer, Concealment, Disguise
- Stock
- Trip
- Travel
- Cruise
- Airplane ticket
- Ticket
- Train ticket
- Deal
- Bank account

Investigation/Audit
- Audit
- Auditor
- Auditor General
- State Auditor
- Investigation
- Investigator
- Special Agent
- Prosecutor
- Summons
- Subpoena
- Evidence
- Interview

Cover-up/Tampering
- Hidden
- Corrupt
- Secret
- Covert
- Cover up
- Cover-up
- Conspiracy
- Hiding
- Concealment
- Concealed
- Exposure
- Not get caught
- Secret
- Special
- On the QT

and each result must be reviewed in the context of the e-mail, industry, language, case knowledge, and other evidence obtained.

- *Prima Facia Evidence* – The search strings for this category are designed to uncover information relating to actual crimes committed. Included in this string are words such as "bribe," "kickback," "gratuity," "illegal gratuity," and "graft." Depending on the corrupt relationship, this may include terms like "sweetheart contract," "quid pro quo," "fraud," and "crime."
- *Improper Business Relationship* – Mirroring the elements of Title 18, Section 208, this addresses a subject having a substantial relationship in a business venture or negotiating post-government employment opportunities. The successful search might include words like "job," "title," or "job duties." It may also include the name of the job, such as "vice president" or "consultant." Another common method is a no-show job, similar to the one for the wife of a prominent Maryland state senator;[17] terms could include "separation payment," "future opportunity," "my next job," "salary," "employing [name of spouse or relative]," and "job for [name]."
- *Specific Case Issues/Identities* – Depending on the case or investigation-specific information already obtained, searches can be made on these items. For example, if a "quid pro quo" involved hiring a target's cousin, that name should be searched. Other examples may include business names, titles (see above), bank accounts, travel destinations, etc.
- *Cash Exchange* – Currency deposits, exchanges, and similar actions are red flags of illicit activity and search results that indicate significant banking activity must be investigated. In drug and terrorism cases, this is an important indicator, as well as in public corruption cases. For example, recently convicted Louisiana congressman William Jefferson placed his cash "on ice," by literally hiding it in his freezer.[18] Strings to search may include "cash," "money," and "consulting fee." Consulting "fees" and "overpaying" a credit card balance are also commonly used to hide the source of illicit funds.[19]
- *Asset Transfer, Concealment, or Disguise* – In the Cunningham case, the congressman was paid with assets, mainly boats and residences.[20] Significant assets that may be "loaned," given, or transferred, through third-party owners (to disguise their source) and could be located with search terms such as "boat," "motorcycle," "plane," "aircraft," or any other type of asset given. Other terms used include "hidden owner," "hidden ownership," "secret," "transfer," "special," or phrases like "just between us" or referring to the "gift" given to the individual.
- *Investigation or Audit* – After she joined Boeing, Darleen Duryun complained in e-mails to Boeing's CFO that she had been contacted by a company attorney conducting an internal investigation regarding her hiring. She asked the CFO for advice on "what to say."[21] This type of e-mail correspondence could be indicative of a problem. Terms: "audit," "auditor," "investigation," "investigator," "special agent," "Special Agent [specific name]," or terms that could indicate an on-going investigation, like "evidence," "subpoena," "search warrant," "summons," "prosecutor," and "interview." Another significant issue that may be located is the fact that most officials are required by law to report their assets, income, gifts, and other financial information on a financial disclosure form. The Ethics in Government Act of 1978 requires this for all federal officials and employees in sensitive positions. Terms that are alerting in this situation are "financial disclosure form," "financial disclosure," or "ethics probe."
- *Cover-up and Tampering* – Since corruption is a two-part crime, naturally, a conspiracy forms. Similar to the investigation/audit search terms, cover-up or tampering language is another red-flag that could lead to prosecution based on several additional statutes, witness tampering, destruction of evidence, etc. Search strings for this category include "secret," "don't talk," "don't tell anyone," "just between us," "conspiracy," "coverup," "cover-up," "hush up," or "hush money."

It should also be noted that the search terms given here are examples, and the full list of terms should be carefully brainstormed and evaluated by the investigator, examiner, and case supervisor prior to conducting the actual search. E-mails are not the only place for hiding information, and all documents, web searches, and other evidence – paper and digital – should be examined properly for any additional leads or corroboration. Electronic searches also need to determine if the target uses a third-party online file storage site.[22] The fraud investigator or computer examiner should have a working understanding of the crime they are searching for. For pub-

17 United States v. Thomas L. Bromwell, Sr. Plea Agreement, dated July 20, 2007. http://www.washingtonpost.com/wp-srv/metro/BromwellThomasPlea.pdf

18 United States v. William Jefferson. Indictment, dated June 4, 2007. http://media.washingtonpost.com/wp-srv/politics/documents/jefferson_indictment_060407.pdf

19 *Supra* note 3, at 1.706

20 *Supra* note 2

21 *Supra* note 12

22 Communication with Thomas Talleur, July 2008

Common Hiding Places for Corrupt Payments & Transfers

- Currency hoards
- Cashiers and travelers checks
- Deposits to financial institutions
- Financial investments (commodities, securities, stocks, bonds)
- Business Investments (on- / off-book schemes, dissolved corporations, bookkeeping devices for concealment)
- Real property investments
- Loans to friends, business associates, and relatives
- Overpayment of taxes
- False debts and false lawsuits/ judgments
- Gifts and fraudulent conveyances
- Trusts
- Purchasing assets or spending proceeds
- Insurance policies (equity)
- Debt pay-off (credit cards/ mortgage payments)
- Proceeds: drugs, alcohol, sex, gambling, travel

lic corruption, money laundering, white collar crime, and fraud investigations, there are two issues: 1) where the money is hidden, and 2) how it was transferred.

CONCLUSION

Several recent cases illustrate the effect of electronic mail and correspondence in fraud and corruption cases. A *Wall Street Journal* article on a failed subprime mortgage suspected of fraud was identified by Wall Street banks as being a problem long before it failed; the analysts documented their concerns in e-mails, which was then subpoenaed by the Bankruptcy Trustee.[23] In Baltimore, Mayor Sheila Dixon resigned in disgrace in January 2010, after a long and public probe into public corruption. She was convicted of purloining gift cards meant for the poor. While a second trial on perjury for allegedly lying on financial disclosure forms was disposed of in her plea, an affidavit submitted for a search warrant of her home specifically described e-mail communications between her and a lover/ city developer regarding travel and gifts, which she failed to report on her ethics forms. [24]

E-mail evidence is critical in all criminal investigations and can help prove intent. Public corruption cases are the most difficult, because of the reputations and power of the defendants. Such cases are also the most damaging for the citizenry to understand, since it erodes public confidence of and support for, public functions. As the old saying goes, "absolute power corrupts absolutely." Elected and appointed government officials sell their soul when they agree to a corrupt relationship.

As Benjamin Franklin so aptly put it, "there is no kind of dishonesty into which otherwise good people more easily and frequently fall than that of defrauding the government." We expect our public officials to act in the best interest of the community, not for personal enrichment. When this happens, it constitutes such a grave blow to our combined sensibilities that we must act.

This protocol was designed to ensure that investigations into public corruption do not neglect the large and rich amount of evidence likely contained on a hard drive or e-mail server. By using an organized procedure, the investigator and examiner will be more successful, more efficient, and better understand the case they are investigating. ❧

23 Wall Street Journal, "Banks Doubted Lendor, but Still Propped it Up." Steve Stecklow, November 10, 2009. http://online.wsj.com/article/SB125771933475937109.html

24 Baltimore Sun. "Sun Coverage: City Hall Investigation" http://www.baltimoresun.com/news/local/baltimore_city/bal-council-probe,0,1060673.storygallery

Colin May

Colin May is an investigator with the U.S. Department of Defense. He joined the federal service in 2002, when he became an intern with the Export-Import Bank of the United States; the following summer, he worked for the Bureau of Citizenship and Immigration Services for the U.S. Department of Homeland Security.

After a fall internship with the Postal Inspection Service in Albany, N.Y., he graduated with a bachelor's degree in marketing/ management from Siena College and worked for the International Association of Chiefs of Police before re-joining the government. In 2006, he became a certified fraud examiner.

He received a master's degree in forensic studies from Stevenson University in 2008 and a graduate certificate in forensic accounting from Northeastern University in 2009.

[INVESTIGATIONS]

Inspectors General Supreme Impact

On a more personal note, I felt honored to be able to attend the full hour-long Supreme Court hearing of the case

By Brian Haaser

It is rare for the U.S. Supreme Court to hear a case that directly impacts investigative work done under one's own jurisdiction as an Office of Inspector General investigator. However, during my 31-year career as an investigator for the Department of Agriculture OIG, I have witnessed it twice. The first instance—a case involving food stamp fraud—centered on determining whether the government had to prove that the defendant knowingly committed a crime: was ignorance of the law an excuse? The second instance—a still-undecided case [1]concerning dogfighting videos—focuses on the limits of free speech: are commercial images of animal cruelty a protected form of expression? While we in the inspector general community know that our investigations have deep programmatic and personal significance, we should also keep in mind that our work can sometimes impact the law of the land.

Blissful Ignorance or "Guilty Mind"?

In the early 1980s, I was a desk officer at USDA OIG headquarters in Washington, D.C., and was responsible for monitoring food stamp issues that could impact our investigative work. In one case that I was following, the co-owner of a store had illegally bought a total of $1,195 in food stamps for $800 in cash from one of our undercover agents. In food stamp fraud, people generally buy the benefits below their face value and then redeem them later with the government for their full worth. The store—a sandwich shop—was not authorized to take food stamps, so this seemed like an open-and-shut case. It was not.

The law states that a person who "knowingly uses, transfers, acquires, or possesses [food stamps] . . . in any manner not authorized by [the statute] or the regulations," shall be guilty of a criminal offense.[2] According to the defendant, this wording meant that the government had to prove that he knew he was violating the law, not just that he had violated the law. In legal terminology, this is called proving "specific intent" or *mens rea*, Latin for "guilty mind."

The district court judge saw it differently, however, and—over the defendant's objections—instructed the jury that the case turned on proving that (1) the store owner had bought the food stamps illegally, and (2) he had knowingly and willfully bought them. Whether or not the owner knew he was violating the law, he had indeed violated it; guilty-minded or innocent-minded, his mental state did not matter.

So instructed, the jury convicted the owner. The owner appealed the case on the basis that the district court judge should not have refused to instruct the jury that "specific intent" is required in a prosecution under the statute. However, the appeals court agreed with the original

1 After this article was written the United States Supreme Court issued its ruling on United States v. Stevens regarding 18 U.S.C. § 48, on April 20, 2010. In an 8 to 1 decision, the Court struck down the law, stating "Section 48 is not so limited but is instead substantially overbroad, and therefore invalid under the First Amendment." The law is no longer enforceable unless Congress revises it to meet the standard set by the Courts.

2 The Food Stamp Act of 1964 § 14, 78 Stat. 708 (1964) (current version at 7 U.S.C § 2024(b)(1) (2009)).

judge's rationale.

By 1985, the case had made its way to the U.S. Supreme Court, which agreed to review it because the appeals court's decision conflicted with recent decisions by three other appeals courts. The Supreme Court described the question at hand as being "whether in a prosecution under this provision [of the statute] the government must prove that the defendant knew that he was acting in a manner not authorized by statute or regulations."[3] For the court, which overturned the conviction, the answer was yes.

The ruling rested chiefly on two points. First, the law was ambiguous as to whether "knowingly" applied solely to knowledge of the action itself—acquiring food stamps—or also to knowledge of its being illegal ("in any manner not authorized"). Without evidence in the statute of clear congressional intent, the Supreme Court kept to its longstanding principle of leniency in such cases. Second, the court found that the effect of the government's interpretation would be to "criminalize a broad range of apparently innocent conduct." For example, food stamp recipients who bought food from a store that charged them higher prices than normal would be criminals, even if they were unaware of the markup.[4]

Although the Supreme Court's ruling was narrowly restricted to food stamps—you cannot get out of a speeding ticket by saying you did not know the speed limit—I believe that the decision's general principles merit consideration by the investigations arms of other OIGs. Although investigators are not lawyers, our investigative techniques, evidence gathering, and general approach depend heavily on exact legal interpretations. We must make sure that we are investigating precisely the crime that the law articulates, and that we are gathering just the evidence needed to prove that the law was violated.

For USDA OIG, the ruling meant that we had to alter our standard investigative procedures for food stamp fraud cases. We now obtain documents proving that our suspects received USDA's educational material about what is and is not allowed in the food stamp program. We interview witnesses to confirm that our suspects knew it was illegal to buy food stamps. And during our undercover operations, we worked to record suspects acknowledging their crimes.

On a more personal note, I felt honored to be able to attend the full hour-long Supreme Court hearing of the case. I had been to the court before as a member of the public, for the permitted five minute increment, but this was the first time I was able to hear a case argued in its entirety. I was struck by the audience's silence. The room was quieter even than for federal court cases; we wanted to hear every word, follow every argument, and understand every nuance of this institution that holds the power to make decisions that can change our country. I was proud and privileged to be a small part of that process, not once, but twice.

Freedom of Speech or a "Cruelty Thing"?

Unlike with food stamp fraud, the law is clear about the role of intent when it comes to selling images of animal cruelty: "Whoever knowingly creates, sells, or possesses a depiction of animal cruelty with the intention of placing that depiction in interstate or foreign commerce for commercial gain, shall be fined under this title or imprisoned not more than five years, or both."[5] There are exceptions when the image's value is not strictly commercial—for example, if it has significant scientific or historical value—but if a person is just trying to profit from something that shows animals being treated cruelly, then he or she is a criminal. Or, as I recently found out, maybe not.

The law on depictions of animal cruelty was not written specifically to stop people from selling dogfighting videos. As the congressional testimony and legislative history show, it was passed to stop a type of fetish video known as a "crush video" from being distributed.[6] "Crush videos" depict small animals being stepped on, usually by women in high heels or bare feet. The tortured cries

3 Liparota v. United States, 471 U.S. 419, 420-421 (1985).
4 Id. at 426.
5 18 U.S.C. § 48 (2009).
6 See 145 CONG. REC. 10685 (1999); See also 145 CONG. REC. 25,893 (1999).

of the animals are sometimes accompanied by a kind of dominatrix patter from the women. In 1999, "crush videos" provided the impetus for Congress to make depictions of animal cruelty illegal for interstate sale.

Under the 1999 law, I supervised a 2003 investigation that initially seemed straightforward. A Virginia man's home business, Dogs of Velvet and Steel, sold dogfighting videos and related merchandise across State lines. Led by USDA OIG, this joint investigation also involved the U.S. Postal Inspection Service and the State police departments of Virginia and Pennsylvania.

In January 2003, a USDA OIG special agent and a Pennsylvania State police investigator responded to an advertisement by Dogs of Velvet and Steel in an underground dogfighting magazine. They purchased several videotapes and items of dogfighting paraphernalia and arranged for them to be sent from Virginia to an undercover address in Pennsylvania. After receiving the items, we obtained a warrant and seized the business owner's stock of videotapes, books, periodicals, and training equipment, as well as his customer lists and financial records. We were able to show that in total, the business had derived $57,000 from selling dogfighting merchandise during the previous two years.

The dogfighting equipment included items such as "break sticks," which are used to pry apart fighting dogs' jaws when they lock their teeth into each other. There were also magazines, books, and videos of dogs training, fighting, and killing other animals. In some of the videos, the business's owner took the role of a sports announcer, narrating dogfights and then offering his post-fight analysis. In another video, he described the action as domestic pigs were released, chased down, and killed by trained fighting dogs—noting at one point: "We are getting into a cruelty thing here."

We set up our investigation to show that all the major elements of the law had been violated. The graphic videotaped violence was a clear example of animal cruelty. Mailing the videos and other material was a clear example of engaging in interstate commerce. The money earned from these sales proved commercial gain. Together, the owner's placement of an advertisement, delivery of merchandise, and acceptance of money showed his intention to profit from depicting animal cruelty. The U.S. attorney's office agreed and decided to prosecute.

In January 2005, the case went to trial. The evidence we gathered was sufficiently solid that the defense's strategy was not to question whether the defendant had violated the law, but instead whether the law violated the Constitution. The First Amendment states that Congress shall make no law "abridging the freedom of speech," which has been understood to include books, images, and other depictions such as video. Accordingly, the defense argued that the defendant's dogfighting merchandise was protected by the Constitution and that the law itself was illegal. Further, the defense held that the videos had historical value. This suggests that the defendant should be thought of more as a documentary filmmaker than as someone profiting from an animal's pain; the videotaped events are cruel, but—according to this line of thought—the tapes serve as valuable historical records of a distasteful practice.

The federal district court, however, denied the defense's motion to dismiss the case on these grounds. After a three-day trial, the jury deliberated for about 45 minutes and then returned with a guilty verdict. In April 2005, the defendant was sentenced to 37 months in prison; he immediately appealed.

In October 2006, a court of appeals heard the case. The government argued that depictions of animal cruelty should not be protected by the First Amendment and instead should be a prohibited category of speech like child pornography, which the Supreme Court had decided was not protected under the Constitution. The appeals court did not agree, ruling:

> "The Supreme Court has not recognized a new category of speech that is

unprotected by the First Amendment in over twenty-five years. Nonetheless, in this case the government invites this court to take just such a step in order to uphold the constitutionality of 18 U.S.C. 48 [the animal cruelty statute] and to affirm conviction. . . . Moreover, because we agree with [the owner of Dogs of Velvet and Steel] that 18 U.S.C. 48 is an unconstitutional infringement on free speech rights guaranteed by the First Amendment, we will vacate his conviction."[7]

According to the appeals court, the Constitution protected from infringement, the business's right to sell depictions of animal cruelty across state lines.

In December 2008, the Department of Justice asked the Supreme Court to review the case. The court accepted, and the issue attracted heated interest. Twenty-two different organizations—among them the Humane Society of the United States and the National Coalition Against Censorship—filed amicus curiae ("friend of the court") briefs on behalf of one side or the other. (Such briefs lay out legal, factual, or social issues to deepen the court's understanding of the matter at hand). In October 2009, the court heard the case; it is expected to deliver a decision sometime in 2010.

If the Supreme Court finds that animal cruelty depictions are a prohibited class of speech, then OIGs nationwide may have to expand their investigative practices. Although USDA OIG is responsible for investigating animal cruelty cases, other OIGs could have another avenue of employee misconduct to pursue if government equipment is used to make, view, or distribute such images. In effect, the Supreme Court's ruling may broaden agencies' power to regulate speech in the workplace, which in turn would broaden our responsibility to investigate related violations. Having depictions of animal cruelty on work computers would become as illegal as having child pornography.

On the other hand, if the court agrees with the defendant, then an OIG investigation will have led to a U.S. law being overturned; what Congress once outlawed will become not only legal, but a fundamental American right that must not be infringed.

The Supreme Court hears only about one percent of the cases presented to it each term.[8] So, being a witness to one investigation that winds up in the court is rare; being a witness to two is extraordinary. Although each case had small beginnings—$1,195 worth of food stamps and a few items of mail-order merchandise—they both ended up having much larger repercussions. What is the role of criminal intent? How far does the freedom of speech go? Although we as OIG investigators may not know it at the time, any given investigation may ultimately yield answers that will help define us as a nation.

7 United States v. Stevens, 533 F.3d 218, 220 (3rd Cir. 2008), cert. granted, 129 S. Ct. 1984 (2009).

8 The Justices' Caseload, http://www.supremecourtus.gov/about/justicecaseload.pdf

Brian Haaser

Brian Haaser is currently the special agent-in-charge of the Northeast Region, Department of Agriculture Office of Inspector General. Mr. Hasser's responsibilities include managing the investigative program for OIG in 13 states and the District of Columbia (from Virginia to Maine).

Mr. Haaser has been a criminal investigator with USDA OIG from 1979 to the present. He has extensive experience in conducting and supervising criminal investigations regarding USDA related programs to include organized illegal animal fighting ventures; regulatory programs to include illegal import of live animals, agriculture products and pests, issues affecting the meat and poultry industry, and illegal activities involving the grading and wholesomeness of agricultural products; feeding programs for the poor; loan and insurance programs for farmers and businesses; and crimes affecting USDA personnel to include bribery, embezzlement, and assault.

[EVALUATION]

The Postal Service's Share of CSRS Pension Responsibility

Freeing the Postal Service from unjustified legacy costs is critical if it is to have the agility needed to face an uncertain future

By Mohammad Adra and Renee Sheehy

When the Post Office Department became the Postal Service on July 1, 1971, there was no change to postal employees' retirement benefits. Employees continued to participate in the Civil Service Retirement System, and the Postal Service continued to make the same contributions that federal agencies did to the Civil Service Retirement and Disability Fund.[1] The CSRS had historically been underfunded by agency contributions. As a result, the Postal Service was required to increase the funding of its employees' pensions several times.

The Postal Service is currently responsible for meeting any CSRS liability for employees who started after 1971. For employees with service both before and after the Postal Service's establishment, the federal government and the Postal Service share responsibility for CSRS pensions. The federal government pays for service through 1971, and the Postal Service pays for service after 1971.

Responsibility for paying the CSRS costs resulting from inflationary salary increases since July 1, 1971, shifted from the federal government to the Postal Service by statute in 1974. In the late 1980s and early 1990s, a series of laws obligated the Postal Service to fund retiree cost-of-living adjustments since 1971.

Even though the Postal Service was making the newly required payments towards funding its CSRS liabilities in full, no one calculated how well it was meeting this goal until the Government Accountability Office drew attention to the issue.[2] The Office of Personnel Management then evaluated the Postal Service's assets and liabilities in 2002 and discovered that the Postal Service would overfund its CSRS obligations by nearly $78 billion unless the required payments were reduced to reasonable levels.[3] The Postal Service's CSRS contributions had earned an interest rate much higher than the 5 percent assumed by OPM, resulting in a large surplus.

OPM established assumptions about how the Postal Service and the federal government would divide the CSRS obligations for postal employees who worked before and after July 1, 1971. Under OPM's methodology, the Postal Service is responsible for all pay increases since 1971.[4] OPM assumes no responsibility for inflationary increases to salaries from the Post Office Department era. In effect, OPM calculates the federal government's share for these employees as if they retired in 1971 at their 1971 salaries.

Under the current OPM system

1 The Postal Reorganization Act, however, did require the Postal Service to pay administrative costs to the Civil Service Commission, the forerunner of the Office of Personnel Management. This requirement was later removed.

2 GAO, *United States Postal Service: Information on Retirement Plans*, (GAO-02-170, December 2001).

3 The amount of the overfunding was initially estimated as $71 billion and later revised to $78 billion. In addition, OPM's estimate made the Postal Service responsible for CSRS military service credits. GAO reported that the overfunding increased to $105 billion if the federal government retained responsibility for CSRS military service credits. The Postal Accountability and Enhancement Act returned the amount the Postal Service had been overcharged for CSRS military service credits to the Postal CSRS Fund.

4 This allocation of CSRS liabilities concerns employees with service prior to 1971.

for federal retirees, CSRS retirees receive a percentage of their highest 3-year average salary for every year they served. Thus, the critical factors for determining the size of the annuity are years of service and the high-3 salary. The fact that lower salaries were received early in an employee's career is irrelevant to the final pension calculation, because salaries increase throughout that career. This method of calculating the annuity is highly suggestive that years of service is the appropriate basis for allocating CSRS pension responsibility.

The U.S. Postal Service Office of Inspector General commissioned the actuarial firm Hay Group to review the allocation of CSRS liabilities between the Postal Service and the federal government. The report, *Evaluation of the USPS Postal CSRS Fund for Employees Enrolled in the Civil Service Retirement System*, describes the results of Hay Group's analysis.

Several key points emerge from the report and the OIG's analysis:

- OPM's use of years of service and the high-3 salary as the basis for determining CSRS pension benefits strongly suggests that responsibility for CSRS pension payments should be divided between the Postal Service and the federal government based on years of service.
- The current methodology used to allocate CSRS obligations for employees with service prior to July 1, 1971, is not based on years of service and is inequitable to the Postal Service. For example, Hay Group shows how the Postal Service could be responsible for 70 percent of the pension of an employee who worked only 50 percent of his or her career for the Postal Service.
- Every time postal employees receive a pay increase, their CSRS benefits, including any earned at the Post Office Department, grow in value. The Postal Service must pay for this increase not only for post-1971 service, but also for the years of service before 1971. An allocation methodology that assumes employees will receive no pay increases — not even to offset inflation — is not reasonable.
- Furthermore, had new pension plans been created for postal employees on July 1, 1971, and the Postal Service made responsible for all liabilities, it would have paid less than under the current methodology. The Postal Service would not have had to fund the additional liability that results when a pay raise increases the value of the years of service performed for the Post Office Department.
- It is instructive that OPM uses a years-of-service methodology to allocate the cost of retiree health care premiums for retirees who split their careers between the Post Office Department and the Postal Service.
- Allocating pension responsibility on a years-of-service basis would align the pension methodology OPM uses with the methodology OPM uses for retiree health care obligations. Currently, they are at odds with each other as they are applied to the Postal Service.
- Had the more equitable years-of-service allocation methodology been used to determine the value of the Postal CSRS Fund, the OIG estimates its value on September 30, 2009, would have been approximately $273 billion rather than $198 billion — a difference of $75 billion.[5]
- It has been determined that a $10 billion unfunded liability currently exists for the CSRS pension fund. Reducing the $75 billion overpayment by $10 billion still leaves a $65 billion surplus.
- If the $65 billion pension surplus were transferred into the Postal Service Retiree Health Benefits Fund and combined with the $35 billion already set aside, the total value of the health benefits fund would grow

5 Hay Group estimates the difference in the value of the Postal CSRS Fund as of September 30, 2006, to be $58.7 billion. The OIG's estimate extends Hay Group's analysis to 2009. Both estimates only measure the change in the value of the Postal CSRS Fund and do not include the reduction in liability from allocating a smaller share of CSRS payments to the Postal Service in the future. This change in liability would further increase the Postal Service's CSRS surplus.

to $100 billion. Moreover, even at 5 percent interest, the balance of the fund would increase $5 billion or more each year.

- The $100 billion balance in the retiree health benefits fund would be more than sufficient to cover the $87 billion OPM estimates the Postal Service has accrued in retiree health care liability as of the end of 2009. No further payments to the fund would be needed to cover this liability.
- Since all of the Postal Service's accrued liabilities for retiree health benefits would be fully funded, the seven remaining annual payments to the retiree health benefits fund, which average $5.6 billion each, could end.
- In addition, Postal Service payments for the health benefit premiums of current retirees could start coming from the retiree health benefits fund immediately.
- The annual evaluation of the Postal Service's retiree health benefit assets and liabilities would continue, and the Postal Service could be assessed if there were any future unfunded liability.

The Postal Service was intended to be an independent, self-sufficient entity, yet during the period when postal rates were set to cover costs, citizens and businesses were charged far in excess of what was needed to fund CSRS benefits. Today, the Postal Service continues to be assigned an unfair share of CSRS liabilities. Postal ratepayers should not be burdened with federal liabilities. Instead, they should be credited for their previous overpayments. Ending the unfair allocation of CSRS liabilities would result in a CSRS surplus that could be used to fully discharge accrued retiree health care liabilities. This would put the Postal Service on a sound financial footing. All of its current obligations to its retirees (both pension and health care) would be fully funded.

Freeing the Postal Service from unjustified legacy costs is critical if the Postal Service is to have the agility it needs to face an uncertain future. A new, equitable CSRS cost allocation methodology should be established based on years of service. The resulting CSRS surplus can then be transferred into the retiree health benefits fund. Such a transfer is not unprecedented. A similar transfer happened in 2007 and is scheduled to occur for any CSRS surplus in 2015. ❧

Mohammad Adra

Mohammad Adra is the assistant inspector general for Risk Analysis Research Center for the U.S. Postal Service Office of Inspector General. He has been with the OIG since 2002. Prior to his OIG tenure, he worked five years for the US Postal Service in pricing and five years for the Energy Information Administration in energy demand forecasting.

As the assistant inspector general, Mr. Adra is responsible for research and data mining activities geared toward assessing risks and producing research papers on applied public policy, economic analysis, and strategic issues pertaining to the Postal Service. The research and data mining activities conducted by his office also support the work of the Office of Audit and the Office of Investigation.

Mr. Adra received his master's degree in applied economics from John Hopkins University and an MBA from Humboldt State University. He also received his bachelor's degree in mathematics from the University of Colorado.

Renee Sheehy

Renee Sheehy is an economist with the Risk Analysis Research Center, U.S. Postal Service Office of Inspector General in Arlington, Va. Before starting with the OIG in 2005, Ms. Sheehy was with the Postal Rate Commission for eight years. She is a member of Risk Analysis Research Center.

For the Risk Analysis Research Center, she has worked on projects related to health and pension funding and the Postal Service's retail network. She has also assisted with the Office of Inspector General's blog.

Ms. Sheehy received her bachelor's degree in medieval studies from Georgetown University, a master's degree in medieval studies from Catholic University and she is currently working on her masters in economics at George Mason University.

[OUTREACH]

Training an Ex-Communist Country on the Inspector General Concept

Members of our audience understood that we shared their struggle to ensure the integrity of government programs

By Dennis A. Raschka

In September of 2009, the U.S. Department of Justice invited representatives from four Offices of Inspector General to deliver a three-day symposium in Kiev, Ukraine, on how the Inspector General Act is implemented in the United States. Presentations were given on the process of conducting audits, criminal investigations, evaluations and inspections, and hotlines. At the end of the symposium, the presenters and the attendees learned about the huge challenges facing Ukraine's small cadre of auditors and investigators in bringing integrity to a nation that had been under communist rule until 1991.

The Invite

In March 2009, DOJ arranged for a delegation of Ukrainian officials to visit five OIGs in the United States. We, at the Department of Housing and Urban Development OIG, were contacted by DOJ's Office of Overseas Prosecutorial Development, Assistance, and Training. The office had been working with the Ukrainian government ministries to assist them in the development of internal investigative units that were envisioned as inspector-general type offices. The work of the office focused on fighting corruption within the Ukrainian government and was part of a larger effort under the Millennium Challenge Corporation's Threshold Country Plan – a grant made through agreement with the government of Ukraine. To coordinate efforts in Ukraine, OPDAT incorporated resident legal advisors that were highly experienced DOJ attorneys and experts on anticorruption measures. Rob Storch and Bohdan Vitvitsky were among the two U.S. attorneys that worked extensively on this program in Ukraine.

Of the two Ukrainian ministries that visited the United States, neither had traditional law enforcement powers. As a result, Rob Storch asked us to focus on what could be done with regards to internal auditing, program review, and investigation in criminal cases, once they are turned over to those with jurisdiction in their areas.

In our presentation, we covered the basics of the Inspector General Act and gave a brief overview on the types of audits and investigations we conduct, and our hotline – the operation in which the majority of our visitors were keenly interested in learning. We learned that the Ukrainian ministries had also visited three other OIGs: the Department of Agriculture, Amtrak, and the Department of Transportation. At the conclusion of the presentations, we bid farewell and assumed that was the end of our business with Ukraine. A few months later, HUD Inspector General Kenneth Donohue received a letter from DOJ inviting representatives of our office to go to Kiev, Ukraine, to conduct a symposium on U.S. Inspector General activities. The inspector general accepted the

invitation, and arrangements began for four members of our staff to attend. We learned from Rob Storch that staff members from three other OIGs and a retired HUD OIG employee[1] were also invited.

Planning

During the summer, the group coordinated on an agenda and worked out assignments for the presentations. Rob Storch and Bohdan Vitvitsky provided insight into the political and operational realities of conducting anticorruption efforts in Ukraine.

For example, kickbacks were an established way of conducting business and even extended into the judicial system. As for audits, they were merely accounting exercises – if the books balanced, that was sufficient. There were also separate audit and investigative units. An organization that combined all of these functions was alien to the Ukrainians. Audits seldom questioned document authenticity, cost eligibility, or indications of fraud. As a case in point, the Ukrainians had a hard time understanding why Americans had to prove eligibility for basic services such as housing vouchers, food stamps, and welfare.

In the Ukrainian system, these were rights given to all citizens. We also worked under tight deadlines to get our powerpoint presentations completed in advance so they could be translated.

The Symposium

The symposium began on September 15, 2009. Among the topics covered were presentations on public corruption in the United States and case studies of audits, investigations, and inspections. Our presentation took place in a theater and we spoke to 250 attendees from six different ministries. Rob Storch and Bohdan Vitvitsky had arranged for simultaneous translations of all presentations.

As we spoke into the microphones, translators would immediately translate our words to Ukrainian via a wireless sound system. Attendees wore portable earphones to help them hear the translations. When there were questions, the process was reversed and presenters heard the Ukrainian questions translated to English.

Overall, the translation was a smooth process, except in instances where some were quite literal, and we had to avoid idioms the best we could. A few of us found out that some jokes were met with silence because the translations did not pass along the subtleties of jokes based on word play. The Ukrainians' sense of humor is also evidently very different from our own. At other times we scrambled to track where we were in the presentations because our slides on the screen were all written in Ukrainian and we occasionally lost our place. Regardless of these small difficulties, the core message was well-received.

Members of our audience understood that we shared their struggle to ensure the integrity of government programs. Among the topics covered at the symposium were:

- An overview of the audit process to the agents and the investigative process to the auditors.
- A review of audit standards used in the United States.
- An explanation of the types of audits conducted and how audit planning is done.
- Audit methodology and a discussion on how to audit contracts and procurement.
- Auditing payroll and cash.
- Inspections and evaluations that currently are not done in Ukraine.
- Investigative planning and techniques.
- Documentary evidence, and informant development.

Culture Shock

We learned during the symposium that in the investigative arena, some Ukrainian laws are different from the United States due to the country's history and citizen distrust. One instance of this difference is seen with respect to Ukrainian surveillance; many Ukrainian investigators are prohibited from conducting video surveillance without a court order. The investigators explained that this prohibition exists because there is great fear of a KGB – type of atmosphere that existed under Russian dominance. This point was underscored by the fact that our hotel stood two blocks from the building of the Security Service of Ukraine. The Ukrainian security service

Building of SBU (Security Service of Ukraine)

1 HUD OIG staff on the trip included Jim Heist, Assistant Inspector General for Audit; Frank Rokosz, Assistant Director, Technical Oversight and Planning Division, Office of Audit; and Ruth Ritzema, Deputy Assistant Inspector General for Investigation. Other staff included Katherine Moore, Supervisory Auditor; Alan Klein, Senior Director, Office of Audit; and Mike DeJoseph, Senior Agent, from DOT OIG and Colin Carriere, Counsel to the Inspector General/Deputy Inspector General for Investigations, from the Amtrak OIG. Tom Ackerman, Special Agent with USDA OIG, represented the Inspector General Criminal Investigator Academy.

is a cross between our Central Intelligence Agency and Secret Service. Our hosts explained that during the Second World War, the building had served as the headquarters of the Gestapo. People brought into the building would never come back out. After the war ended, the building became the headquarters of the KGB, maintaining the same reputation as the Gestapo. The current Security Service of Ukraine is the successor to the KGB and is still controversial as it is suspected of illegal surveillance and eavesdropping. This situation has made it difficult for legitimate law enforcement to develop and gain a level of trust or cooperation that is enjoyed in America.

The situation is also further complicated as Ukraine is considered one of the top countries in the world for public corruption. Previous studies by the U.S. Agency for International Development and the Atlantic Council (a U.S. citizens group formed to promote the Atlantic Treaty Association, which supports the North Atlantic Treaty Organization) report that public corruption is deeply ingrained within Ukraine. Bribes and political payoffs are common. The studies call, among other actions, for Ukraine to adopt an Inspector General unit in each ministry and pass stronger anti-corruption legislation.

Symposium Close

Both the audit and investigation breakout sessions concluded with practical exercises on the material. Participants completed the symposium by presenting their solutions to the case studies. They also took the case studies seriously and gave creative answers, even challenging the instructor's solutions.

The finale was a presentation on how to set up a hotline. This exercise generated many questions. Ukraine has a unique law that specifies only written complaints can be accepted, and those must be responded to in writing. Phone and e-mail complaints are not considered valid complaints, and participants were seeking ideas on how to deal with that restriction. Participants were also interested in complaint intake and tracking systems. The symposium ended with the presentation of certificates to each participant.

Kiev

Following the sessions, we toured the city. It is a beautiful place overlooking the Dnieper River. Kiev is dotted with many gold-domed churches. Its unique architecture and friendly people make for a small town feel even though it has a population of more than 3 million. The history of Kiev goes back to 966 A.D. However, the city has a long history of invasions and occupations. Ukraine celebrates two independence days, which do not include its recent break from the Soviet Union. We were about 100 miles from Chernobyl, a place we would have liked to visit had time permitted.

Conclusion

All OIG instructors learned that Ukraine is seriously seeking ways to reduce the corruption that affects the operations of its society. Although we like to think that the U.S. Inspector General model can be universally adopted, it is obvious that doing so will require special adjustments due to the culture and laws of the country. Thanks to the Millennium Challenge Corporation, we were afforded an opportunity to share the U.S. Inspector General model and our experiences in uncovering fraud, waste, and abuse to Ukraine. We are grateful to our main hosts Rob Storch and Bohdan Vitvitsky. Although this grant has ended, we send best wishes to our new friends in Ukraine and hope that we have helped them be successful in setting up their new units.

Dennis A. Raschka

Dennis A. Raschka has served in the Department of Housing and Urban Development Office of Inspector General for over 35 years. Mr. Raschka started his career as an auditor in Kansas City and later moved to Washington D.C. He has served as the director of the Fraud Control Division, and the Management Information Division. Mr. Raschka was selected as assistant inspector general for Management and Policy from 2003 to 2009. He subsequently retired and then returned to the OIG as the executive assistant to the Inspector General.

Mr. Raschka is the recipient of many commendations and special achievement awards including HUD Distinguished Service Award for his work in developing a Tenant Integrity Program. He was also awarded the IG Special Recognition Award for his work on income computer matching legislation and piloting computer matching at HUD. In 2001 he received the OIG's highest recognition, the Charles Haynes Memorial Award. Mr. Raschka has also received a Meritorious Presidential Rank award. Mr. Raschka received his degree in accounting from Valparaiso University in Indiana.

[OVERSIGHT]

Inspectors General: Prioritizing Accountability

IGs have become accepted as legitimate overseers of government operations, but they remain the subject of considerable debate

By James R. Ives

Retaining the public's trust requires holding government representatives accountable for actions, decisions, and mistakes. Since our nation's inception, Congress and government executives have struggled to design effective mechanisms that can be utilized to ensure accountability. Ensuring public servants are held accountable to multiple parties – to include the president, Congress, and the public at large – is no easy task. The extent to which governance has taken on new proportions and grown more decentralized throughout the past half-century has made ensuring accountability even more difficult. According to Paul C. Light:

> The past half-century has witnessed a slow but steady thickening of the federal bureaucracy as Congress and presidents have added layer upon layer of political and career management to the hierarchy. There have never been more layers at the top of government, nor more occupants at each layer. Information must pass through layer upon layer before it reaches the top of the hierarchy, if it reaches the top at all, while guidance and oversight must pass through layer upon layer on the way to the frontlines, if it ever reaches the frontlines at all. It is little wonder that no one can be held accountable for what goes wrong or right in government, especially in a hierarchy where presidential appointees serve for 18-24 months on average, and information is often delivered by word of mouth through a process that has come to resemble the childhood game of telephone.[1]

In making this statement, Light echoes the concerns of heralds who warned that government expansion would negatively impact leaders' ability to guarantee accountability. For example, President Thomas Jefferson warned that, "the true theory of our Constitution is surely the wisest and best . . . (for) when all government . . . shall be drawn to Washington as the center of all power, it will render powerless the checks provided of one government on another, and will become as oppressive as the government from which we separated."[2] Likewise, Henry David Thoreau warned about the dangers of an ever-expanding national government in stating, "That government is best which governs least."[3] Results of international researcher Tero Erkkilä's studies seem to indicate that Jefferson and Thoreau's concerns were well founded. According to Erkkilä, "Changes in Government due to the fragmentation of power and the decline in role and scope

1 Light, Paul C. *Fact Sheet on the Continued Thickening of Government.* July 2004. Washington, D.C. The Brookings Institution. Retrieved November 11, 2009, from http://www.brookings.edu/papers/2004/0723governance_light.aspx.

2 *America's Constitution*, National Center for Constitutional Studies, retrieved November 10, 2009, from http://www.nccs.net/articles/ril20.html

3 *Respectfully Quoted: A Dictionary of Quotations*, retrieved November 10, 2000, from http://www.bartleby.com/73/753.html

of a state have been seen to create situations whereby the traditional means of accountability no longer fully apply."[4]

In 1978, Congress' search for an effective accountability mechanism resulted in creation of an unconventional concept that would significantly alter the government oversight and accountability landscape. With passage of the *Inspector General Act of 1978*, Congress entrenched OIGs within twelve executive branch departments and agencies.[5] The purpose of establishing these offices was to create independent and objective units to conduct and supervise audits and investigations relating to the programs and operations of [federal] establishments, and to provide leadership and coordination and recommend policies for activities designed to (a) promote economy, efficiency, and effectiveness in the administration of, and (b) to prevent and detect fraud and abuse in, such programs and operations.[6] Although creation of the IG system was clearly indicative of Congress' desire to ensure accountability, the concept did not initially receive universal support. In fact, President Jimmy Carter, various executive branch leaders, and the Department of Justice strongly opposed creation of a network of IGs. "Many in the executive branch regarded the OIGs as 'moles' within their agencies, and DOJ believed that the congressional intrusion into executive branch operations was so substantial that it violated the Separation of Powers doctrine."[7] Executive branch criticism diminished subsequent to passage of the IG Act, and the IGs grew in number as the concept became accepted.

Although IGs have become accepted as legitimate overseers of government operations, they remain the subject of considerable debate. Oftentimes, criticisms relate to claims that IGs have failed to appropriately utilize their far-reaching oversight authorities in an effective manner. Pundits are especially critical of the extent to which IGs rely upon *compliance accountability* standards in an attempt to enhance accountability, versus *performance accountability* and *capacity-based accountability* standards.

Government Accountability – Three Basic Approaches

According to Light, there are three basic approaches that can be utilized to foster government accountability:

1. *Compliance accountability*, which involves efforts to ensure government employees' and related actors' (e.g., contractors, grant recipients, etc.) actions conform to specific rules and regulations. Compliance accountability typically involves holding *individuals* accountable for their actions through utilization of punishments and sanctions, correcting problems *after* they occur, and deterrence of inappropriate behavior through publicizing punitive measures. Investigations and targeted audits designed to identify potential fraud, waste, and abuse are typical compliance accountability tools;
2. *Performance accountability*, which involves identification of potential program weaknesses or inefficiencies. Accountability is promoted through utilization of inspections and reviews designed to ensure programs and personnel are performing in an efficient and effective manner. Performance accountability is much more complicated than compliance accountability, as it "has to do with the ability of an agent to produce things of value for the principal at the lowest possible costs in terms of resources utilized."[8] Performance accountability efforts typically involve evaluating and benchmarking performance in order to avoid problems *before* they occur, rather than punishing inappropriate activity after it occurs.
3. *Capacity-based accountability*, which involves overarching, long-term assessments designed to evaluate the extent to which departments and agencies (or governments as a whole) are appropriately "staffed, trained, structured, and equipped" to the extent they can perform in an effective and efficient manner. Capacity-based accountability efforts generally focus on development of "workable programs and responsive structures."[9]

Light argues that the 1978 IG Act is unique in that it is "the only reform statute to combine all three contemporary strategies of accountability" in that it invites "questions of design, implementation, organization, and effectiveness."[10] Although this is the case, IGs have been criticized regarding the extent to which they opt to focus on their compliance role through utilization of targeted audits designed to identify deficiencies typically associated with individual failures; and criminal, civil, and administrative investigations of alleged fraud, waste, corruption, and abuse on the part of government employees, grant recipients, and contractors.

So why is it that some IGs opt to stress their compliance role? In order to answer this question, it is important to take into consideration unique historical and contextual factors that dominated

4 Erkkila, Tero. *Governance and Accountability – A Shift in Conceptualization.* Public Administration Quarterly. 31, 1. April 1, 2007, p. 18.
5 Kaiser, Frederick M. (2008). *Statutory Offices of Inspector General: Past and Present.* Congressional Research Service Report for Congress. Washington, D.C. The Library of Congress.
6 Inspector General Act of 1978. U.S. Code, Title 5, Appendix 3. Pub. L. 95-452, Sec. 1, Oct. 12, 1978, 92 Stat. 1101.
7 Gates, Margaret Jane, Moore, Mark H. (1986). Inspectors-General: Junkyard Dogs or Man's Best Friend? Russell Sage Foundation. New York, NY, p.10.
8 Gates and Moore, p.75.
9 Light, 1993, p.4-15.
10 Light, 1993, p.12.

the late 1970's and 1980's (oftentimes referred to as the OIG's "formative years").

History Matters! The Formative Years

Congress's decision to give the IGs the authority to engage in all three kinds of monitoring was unprecedented. IGs are expected to assure compliance with rules designed to prevent scandals, but they are also tasked with providing information regarding agency performance and capacity.[11] According to Light, IGs "are not forced by structure or mandate to concentrate on short-term compliance as the be-all and end-all of the job," however, limited availability of resources forced early IGs to prioritize from inception. When created, most OIGs were provided with exceptionally lean budgets, which necessitated hiring skeleton crews. Given their far-reaching authorities, prioritization was a necessity.

Path Dependency

Many social scientists and public administration scholars contend that social processes do not evolve in an unconditioned way. Former decisions have an impact upon those that follow. The theory of *path dependency* "assumes that decisions are initially open to revision, but from a certain point in time onwards, decisions taken increasingly restrain present and future choices. As a result, decisions that have been taken in the past may increasingly amount to an imperative for the future course of action."[12] Additionally, historians typically argue that in order to better understand an event, idea, or concept, we should take *context* into account (those things that surround it in time and place and which give it meaning) in order to establish how a development relates to other events and ideas that occurred during the same timeframe. Assuming these theories hold merit, decisions made within the IGs' formative years, many of which were likely impacted by the political landscape, undoubtedly had far reaching impact upon development of institutionalized missions and functions. This being the case, an assessment of the IG system should explore the political setting which existed during the years that immediately preceded - and followed - passage of the IG Act.

The Age of Government Distrust

According to Light, "The definition of accountability in government has remained relatively constant over the past fifty years: limit bureaucratic discretion through tightly drawn rules and regulations."[13] Light indicates that, "Even a cursory review of contemporary public administration textbooks suggests that the dominant definition is one of command-and-control."[14] Passage of the IG Act is frequently attributed to growing calls for government accountability stemming from high-profile scandals that occurred throughout past decades. In fact, creation of one of our nation's first non-statutory OIGs at the U.S. Department of Agriculture in 1962 (preceding passage of the IG Act by 16 years) stemmed from a high-profile scandal involving Billie Sol Estes, a Texas businessman and close associate of Lyndon Johnson who engaged in a massive fraud scheme involving cotton production. [15] Estes swindled the federal government and private parties out of at least $24 million through utilization of false agricultural subsidy claims. He was sentenced to serve eight years in prison, but his conviction was subsequently overturned by the U.S. Supreme Court in 1965.[16] This outcome led to Congressional and public outcry for increased accountability within federal departments that continued well into the 1970s. Throughout the 1970s, additional high-profile scandals developed. Two particularly significant examples include:

1. Release of a top secret report entitled, "United States – Vietnam Relations, 1945-1967: A Study Prepared by the Department of Defense" (commonly referred to as the *Pentagon Papers*) by the New York Times in 1971, which revealed that President Richard Nixon and other government leaders deliberately

11 Light, 1993, p.33.

12 Koch, Jochen, Schreyögg, Georg, and Sydow, Jörg. (July 2, 2005). *Path Dependence and Creation Processes in the Emergence of Markets, Technologies and Institutions.* Free University of Berlin. Faculty of Economics and Business Administration. Berlin, Germany, p.6.

13 Light, 1993, p.12.
14 Light, 1993, p.12.
15 Light, 1993, p.31.
16 Intergovernmental Relations Subcommittee (1966) Operations of Billie Sol Estes: eighth report by the Committee on Government Operations Intergovernmental Relations Subcommittee, House Committee on Government Operations, United States Congress, Government Printing Office, Washington, D.C., OCLC 35

expanded the Vietnam conflict by bombing Cambodia and Laos, and surreptitiously approved other combat. Additionally, the Pentagon Papers revealed that former presidents – to include Presidents Harry Truman and Lyndon Johnson - misled the public regarding various policy decisions involving Vietnam.[17]

2. The burglary into Democratic National headquarters at the Watergate office complex in Washington, D.C., (the "Watergate scandal") and the subsequent cover-up by Nixon and numerous cohorts. Events that followed led to Nixon's resignation on August 9, 1974 (the only resignation of a U.S. president), and eleven convictions of high-ranking government employees and their associates.

Both events seriously eroded citizens' trust in government, and resulted in demands for enhanced accountability and oversight. According to Margaret Jane Gates and Mark H. Moore, the release of the *Pentagon Papers*, the Watergate scandal, and other notorious activities on the part of government representatives throughout the 1970s (e.g., Spiro Agnew's tax evasion plea, the perjury conviction of CIA director Richard Helms, etc.) were given wide publicity, "thereby confirming the public's generalized suspicions" and causing a "general hostility towards government."[18]

The extent to which public distrust developed in the aftermath of the aforementioned scandals – exasperated by increased demands for government accountability stemming from the dramatic increase in the "size, scope, and complexity of government operations"[19] throughout the 1970s – set the tone for debates in Congress, which eventually led to development of the Inspector General concept and passage of the IG Act in 1978. According to Gates and Moore:

> Given the durability, strength, and salience of these concerns among citizens, it is not surprising that Congress acted to combat fraud, waste, and abuse in government by creating a network of specialized institutions. The OIGs symbolize a public value that has widespread public appeal: the interest in assuring taxpayers that their hard-earned money, grudgingly given for public purposes – is well spent.[20]

The Importance of Visibility

The desire to immediately establish visibility likely impacted IGs decision to prioritize compliance accountability. Throughout the late 1970s and early 1980s, programmatic budget cuts were commonplace. In order to retain adequate funding, government agencies – to include the OIGs - needed to exhibit highly-visible, readily-quantifiable results. This factor likely compelled inaugural IGs to attempt to establish measurable "value" by demonstrating an ability to immediately root out fraud, abuse, and blatant corruption of the nature exposed as a result of high-profile scandals. While the importance of performance accountability and capacity-based accountability may have been fully recognized, IGs likely realized that it would have been exceptionally difficult to measure results associated with related initiatives, whereas it is exceptionally simple to measure results associated with compliance-based accountability (e.g. number of arrests, indictments, and convictions resulting from criminal investigations; amount of money returned to the government coffers as a result of criminal fines and sanctions; amount of money recouped through compliance audits that reveal financial discrepancies, etc.). The bottom line is: it is exceptionally difficult to measure the extent to which oversight organizations' performance and/or capacity-based accountability efforts result in a more "efficient and effective" government, whereas it is exceptionally easy to advertise results associated with traditional compliance accountability efforts. As Light puts it, "raw indictment and conviction rates do not require qualifiers and are not open to interpretation. A conviction is a conviction, plain and simple."[21]

A Desire to Remain Apolitical

In addition to a desire to ensure relevance by remaining visible, new IGs had a vested interest in remaining apolitical (recall the IG Act requires IGs to be appointed "without regard to political affiliation"), at least until such time they accumulated a semblance of credibility in the eyes of Congress. According to Light, the IGs were "safest when they stuck to the most traditional concepts of compliance based monitoring, and most vulnerable when they branched into bigger questions of performance or capacity building."[22] As this is the case, inaugural IGs undoubt-

17 Sheehan, Neil. (1971). The Pentagon Papers: as published in the New York Times.

18 Gates and Moore, p.2.

19 Gates and Moore, p.2.

20 Gates and Moore, p.3.

21 Light, 1993, p.210.

22 Light, 1993, p.7.

edly attempted to evade political skirmishes that could potentially result in animosity on the part of Congress or executive branch leaders. Compliance accountability efforts rarely draw negative attention (it would be political suicide for a member of Congress or an executive branch leader to criticize an IG for pursuing prosecution of a government employee who committed a criminal act, was negligent in his or her duties, or engaged in malfeasance), whereas performance and capacity-based accountability efforts are oftentimes highly political, subjective, and controversial.

The desire to remain apolitical likely caused early IGs to avoid political scuffles; however, it would be next to impossible for them to completely ignore the general political climate given their need to prioritize. During the late 1970s, Congress sent a message to the new IGs via the extent to which they increased their focus upon compliance-related issues. According to Light:

> Congress' growing thirst for information also was undeniable. [Joel] Aberbach documented the stunning rise in oversight starting in the mid-1970s, just about the time the IG concept was enacted. According to Aberbach's data, which were based on his careful subject-matter coding of every congressional hearing that was held in odd-numbered, non-election years between 1961 and 1983, Congress conducted 537 days of oversight in 1977, an increase of 268 percent over 1961. Starting at 146 days of oversight in 1961, Congress became increasingly committed to this task, giving 290 days in 1973, 459 in 1975, and peaking at 587 in 1981. As a percentage of all days spent in hearings, oversight moved from 8 percent in 1961 to 18 percent in 1977.[23]

23 Light, 1993, p.51.

The Drift towards Compliance

Path dependency theorists would likely argue that it is small wonder why newly appointed IGs opted to focus almost entirely on compliance accountability versus performance accountability or capacity accountability given aforementioned factors, all of which exerted significant pressures upon IGs during their formative years. Given personnel and resource shortages, IGs were incapable of focusing upon all three forms of accountability, so they likely opted to follow a path that would most likely please Congress, executive branch leaders, and members of the public. Focusing primarily on compliance accountability allowed the new IGs to engage in activities that generated very *visible* results and appeased politicians intent upon convincing constituents that government officials would be held accountable for blatant fraud and abuse. According to Light, "With 535 members of Congress, 270 committees and subcommittees, and almost 3,000 professional staff members as their customers, the IGs had ample incentive to favor compliance monitoring."[24]

Modern Day IGs – Reprioritize or Stay the Course?

Path dependency theory provides one possible explanation as to why IGs continue to embrace their compliance monitoring role but has concentrating on compliance accountability adversely impacted IGs' effectiveness? Does focusing upon compliance monitoring make IGs less capable of ensuring departments, agencies, and individual government employees act in responsible manners? Has the decision to prioritize compliance accountability degraded IGs' ability to effectively oversee government operations? In an attempt to assess the effectiveness of the IGs, Gates and Moore initiated a project which they referred to as a "Performance Inspection of the Offices of Inspectors General."[25] Their goal was to "determine the ultimate value of the IGs" by assessing "exactly how much of the [positive] changes in government performance [they] observed [could be] directly attributed to the IGs."[26] In conducting their study, Gates and Moore note the extent to which focusing on compliance monitoring has led to positive change in that it has resulted in "increased detection of fraud, waste, and abuse; in increased prosecutions and financial recoveries from those who have committed fraud; and in increased rates of audit resolutions and financial recoveries from those agencies that have used government money abusively or wastefully."[27] According to their study, from 1978 through 1983:

- Reported allegations of fraud, waste, and abuse increased from 10,000 per year to over 25,000 per year;
- Successful prosecutions increased from a approximately 1,000 to approximately 4,000;
- Actions against government employees and contractors increased from 700 to 2,500.[28]

Gates and Moore conclude that, "Although there is some uncertainty about the accuracy of these numbers, they do suggest heightened levels of investigative and audit activity."[29] They argue that IG compliance efforts can be deemed successful in that the organizations "seem to be detecting more fraud, waste, and abuse and moving more aggressively to recover losses than their predecessors."[30] Although more critical of IGs' efforts, Light concedes that compliance efforts have not been altogether ineffective. He states that, "From a fraud, waste, and abuse perspective, the IGs have…

24 Light, 1993, p.39.

25 Gates and Moore, p.61.
26 Gates and Moore, p.58.
27 Gates and Moore, p.61.
28 Gates and Moore, p.61.
29 Gates and Moore, p.61.
30 Gates and Moore, p.69.

been effective, if, that is, effectiveness is measured in purely statistical terms. The IGs have accumulated huge savings over the past decade, along with increasing amounts of that visible odium that comes from indictment and conviction of individual wrongdoers."[31]

Although this is the case, Gates, Moore, and Light believe efforts involving performance and capacity-based accountability should increase. Light opines that, "the IGs would be more valuable to their agencies and Congress if they focused less on short-term statistical accomplishments, particularly those involving investigations, and more on program design emerging from outcome-oriented evaluations and inspections."[32] Along those same lines, Gates and Moore note that:

> The President's Council on Integrity and Efficiency and Congress are beginning to see that financial returns to the government of detecting and recovering fraud, waste, and abuse are trivial compared with the potential returns from prevention. Indeed, in accounting for the "total monetary impact" of the OIGs (understood as savings to the federal government resulting from OIG activity), recoveries from past instances of corruption account for less than five percent of the estimated impact.[33]

While this statement seems to indicate Gates and Moore are critical of the extent to which the IGs have focused predominately upon compliance activities (traditional audits and investigations), in reality, they believe IGs are prioritizing consistent with Congressional guidance. Although they recognize the fact that the broad charters of IGs allow them to play diverse accountability roles, they conclude that:

> The OIGs have positioned themselves comfortably within the broad mandate created by Congress. Inevitably, the bulk of their activities remain in the traditional areas of investigation and audit. That is what Congress seems to have intended. It is also consistent with the current capacities of the OIGs. The OIGs have not benefited from any large increases in resources."[34]

Although Gates and Moore are not overly critical of the decision to focus upon compliance accountability, they see value in focusing more on performance and capacity-based accountability in the future. For example, they cite opportunities to "contribute to government performance in terms of proposed administrative changes that would *prevent* fraud, waste, and abuse."[35] However, they also understand that focusing upon performance and capacity-building comes with significant risks and challenges, and warn IGs not to ignore the political environment when engaging in performance and capacity-based accountability efforts. They state that:

> The OIGs seem to face two great risks in influencing government operations. One risk is that they, their interests in promoting financial integrity, and their proposals will not be taken seriously by program managers. Lest one think this unlikely, it is sufficient to point out that all of the cases we studied revealed consistent failures of management to respond to OIG recommendations, which consequently led to problems. A second great risk is that the OIGs will be taken too seriously. After all, as we have seen, the pursuit of financial integrity by itself is not necessarily identical to the concept of accountability, nor to increased efficiency. If the "principals" in Congress, the executive branch, and the courts want products of a certain type and are willing to spend only limited amounts for computers and administrative costs, they may accept some losses in financial integrity without feeling that their "agent" has been unaccountable. The agent may have produced exactly what the principals wanted.[36]

Regardless of the risks associated with expanding their oversight role, IGs may want to at least consider placing increased emphasis upon performance and capacity-based accountability. Many accountability experts have noted the extent to which performance accountability is currently emphasized in government circles. According to Kathryn Newcomer, "Federal managers are currently changing the way they do business in response to a variety of initiatives from both the executive and legislative branches. Signals from the White House contained in the National Performance Review and from the Congress in the *Government Performance and Results Act of 1993* call for managers to focus on programmatic results rather than procedural guidelines as they steer their programs."[37] Given this fact, IGs who fail to place at least some emphasis upon performance and capacity-based accountability may find themselves falling out of favor with two of their primary customers (executive branch leaders and Congress). Newcomer points out the fact that the first National Performance Review (1993) specifically referenced the IGs, and asked them to "broaden the focus of the in-

31 Light, 1993, p.203.
32 Light, 1993, p.194.
33 Gates and Moore, p.60.
34 Gates and Moore, p.58.
35 Gates and Moore, p.69.
36 Gates and Moore, p.69-70.
37 Newcomer, Kathryn. *The Changing Nature of Accountability: The Role of the Inspector General in Federal Agencies.* Public Administration Review. March/April 1998 (58, 2), p. 130.

spectors general from strict compliance auditing to evaluating management and control systems. To implement this mandate, the inspectors general were advised to survey regularly their customers in their agencies, and the line managers and to establish performance criteria for themselves to assess how well they do in improving their agencies' management control systems."[38] The review advised IGs to "measure their own performance in terms of how well they helped *prevent* [emphasis added] fraud and abuse. This perspective urged the inspectors general be held accountable for their proactive results."[39]

Like Gates and Moore, Newcomer is fully aware of the numerous challenges a shift in priorities entails. She recognizes the role path dependency has played in shaping the priorities of IGs to date in stating that, "The culture within both the agencies and the offices of inspector general must change," and notes that it will be extremely challenging for the IGs to "continue their oversight of management's performance, but through a more proactive lens."[40] To successfully accomplish this goal, the IGs will need to move towards a more "consultative approach" whereby they view their respective departments or agencies as partners versus adversaries.[41] Complicating matters further is the fact that IGs' efforts have been impeded by "declining resources and continuing challenges to their independence [that] plague the inspectors general as they strive to please both executive and legislative masters."[42]

Conclusion

According to path dependence theorists, decisions made by early IGs likely set the stage for the development of future priorities, since institutions tend to be persistent and resistant to change. Once set upon a certain trajectory, it is very difficult for an organization to reverse course, even if logic dictates that there is value in exploring alternative manners of conducting business. Since "the set of decisions one faces for any given circumstance is limited by the decisions one has made in the past, even though past circumstances may no longer be relevant,"[43] choices to focus predominately upon compliance accountability during the formative years will likely continue to impact the manner in which future IGs will perceive their role for the foreseeable future unless a precipitating event leads to *path-breaking*, which typically stems from a dramatic incident that forces institutions to abruptly change course. Although it is possible that such an event will cause priorities to shift, history has taught us that dramatic incidents impacting the IG community oftentimes have the opposite effect. The majority of events that previously influenced IGs' priorities involved momentous cases of fraud, waste, and abuse that caused Congress, members of the executive branch, and other relevant parties to demand additional attention be paid to compliance monitoring (e.g., recent high profile bribery and corruption cases involving U.S. military efforts in Southwest Asia, which have resulted in Congress and other parties requesting that DoD IG and other oversight authorities increase compliance accountability efforts). As this is the case, it is far more likely that prominent abuses – and the resulting aftermath – will cause IGs to continue to focus predominately upon compliance accountability unless they are provided significant additional funds earmarked for enhancing performance and capacity-based accountability efforts.

38 Newcomer, p.130.
39 Newcomer, p.130.
40 Newcomer, p.130.
41 Newcomer, p.130.
42 Newcomer, p.135.

43 Praeger, Dave. *Our Love of Sewers: A Lesson in Path Dependence.* Retrieved November 21, 2009, from: http://poopthebook.com/blog/2007/06/15/sewers-path-dependence/.

James R. Ives

James R. Ives currently serves as assistant inspector general for investigative operations at the Department of Defense Office of Inspector General. He oversees domestic and international criminal investigations conducted by the Defense Criminal Investigative Service, the law enforcement arm of the DoD IG.

Mr. Ives has held several leadership positions at DCIS, to include special agent-in-charge of the DCIS Mid-Atlantic Field Office, deputy director of investigative operations, assistant deputy director for national security, and criminal intelligence program manager. He served as a special agent at the DCIS Boston Resident Agency prior to relocating to the National Capital Region.

Prior to joining DCIS, Mr. Ives served with the Immigration and Naturalization Service from 1992 through 1994. He also served as a special agent with the Department of State's Diplomatic Security Service from 1998 through 1999, and as a special agent (reservist) with the Coast Guard Investigative Service from 1999 to 2006, when he received an honorable discharge.

Mr. Ives is an adjunct professor of criminal justice at University of Maryland University College. He holds a Master of Policy Management degree from Georgetown University, and is currently working towards a Doctor of Philosophy degree in Public Administration at Virginia Tech. This article is a condensed version of a research paper he drafted in conjunction with his PhD program.

[SPEECH]

RSA Cyber Security Conference, San Francisco, Calif. March 4, 2010

Together we can find better ways to safeguard our systems and stop those who would do us harm

By Director Robert S. Mueller, III

Good afternoon. I am pleased to be back here in San Francisco.

I recently read a news story about a tailor in Bogotá, Colombia—a tailor who makes bulletproof menswear. He will design the garment to your specifications, and line it with Kevlar sufficient to stop a bullet fired from a .38 caliber pistol at point-blank range.

Some may question whether this is necessary, or extravagant, or perhaps both. But the world has become increasingly dangerous; this man was merely combining the need to stay safe with the desire to look good at the same time.

Of course, my first thought was for the brave but foolish volunteer who wore these clothes during the testing phase. My second thought was that we could use this kind of ingenuity to safeguard our computer systems.

In the early 1990s, we marveled at the potential of the Internet. The risks seemed a world away, and the dangers were largely limited to teenage hackers and identity theft.

Today, the power and pervasiveness of the Internet are evident in the way we communicate, conduct business, and learn. But the risks are no longer a distant possibility. They are right here at our doorstep. And in some cases, they are already inside the house.

Unlike the Colombian tailor, we are not bulletproof, nor can we make ourselves so. But we can work together to line our networks with the equivalent of Kevlar. We can work together to find and stop those who are taking shots at us, and to prevent future attacks.

Almost 20 years ago, here in San Francisco, I read the book entitled "The Cuckoo's Egg," the story of Cliff Stoll—a systems manager at a Berkeley laboratory. He noticed an accounting discrepancy of just 75 cents, and ultimately tracked it to a German espionage ring tapping into our military networks.

I mentioned the story to several FBI employees to illustrate the evolution of cyber crime. And I asked if anyone had read the book.

One reply did stick in my craw. A younger employee said, with what looked like a smirk, "I haven't read it, sir; I was only 10 when it was published." I said, "Thank you for reminding me of how old I am. I am sure you will be very happy in the FBI's Yemen office."

Ancient though it may be, the story of Cliff Stoll illustrates how far we have come, and how quickly.

Today, we will talk about what the FBI is doing to investigate and prevent cyber crime. We will focus on the power of partnerships. And we will touch on what we must do to prevent cyber crime from becoming endemic to our businesses, our economy, and our national security.

Let us begin with cyber threats to our national security. As you well know, a cyber attack could have the same impact as a well-placed bomb.

To date, terrorists have not used the Internet to launch a full-scale cyber attack. But they have executed numerous denial-of-service attacks. And they have defaced numerous websites, including Congress' website following President Obama's State of the Union speech.

A group known as the Iranian Cyber Army claimed responsibility for this attack. And while the damage may have been limited, such groups may attack for publicity or impact, and they are becoming more adept at both.

In the past 10 years, al Qaeda's online presence has become as potent as its physical presence. Extremists are not limiting their use of the Internet to recruitment or radicalization; they are using it to incite terrorism.

Thousands of extremist websites promote violence to a ready and a willing audience. They are posting videos on how to build backpack bombs and bioweapons. They are using social networking to link terrorist plotters and plans.

Of course, the Internet is not only used to plan and execute attacks; it is a target in and of itself. Usama bin Laden long ago identified cyberspace as a means to damage both our economy and our psyche—and countless extremists have taken this to heart.

We in the FBI, with our partners in the intelligence community, believe the cyber terrorism threat is real, and it is rapidly expanding. Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward combining physical attacks with cyber attacks.

Apart from the terrorist threat, nation-states may use the Internet as a means of attack for political ends. Consider what took place in Estonia in 2007 and in the Republic of Georgia in 2008. Wave after wave of data requests shut down banks and emergency phone lines, gas stations and grocery stores, even parts of each country's government. The impact of these attacks left us all aware of our vulnerabilities.

Let us turn for a moment to counterintelligence intrusions and economic espionage.

Espionage once pitted spy versus spy, country against country. Today, our adversaries sit on fiber optic cables and wi-fi networks, unknown and undetected. They may be nation-state actors or mercenaries for hire, rogue hackers or transnational criminal syndicates.

These hackers actively target our government networks. They seek our technology, our intelligence and our intellectual property, even our military weapons and strategies. In short, they have everything to gain, and we have a great deal to lose.

There has been much discussion of late about which nation-states pose the greatest danger of cyber attack. And to a certain extent, that discussion is irrelevant. It may not matter who the attacker is, or whether the motivation is political, ideological, or financial. The information may be bought and sold by anyone, anywhere in the world, whether friend or foe.

The end result will be the same: we will lose our data. We may lose access to our own information. And we may well lose our security.

In recent years, we have witnessed a new trend: the collection of seemingly innocuous information about a company and its employees—from e-mail addresses to power point presentations to notes from meetings. This data not only provides inside knowledge of research and development, business plans, or client negotiations. It can provide entrée to a company's network.

Hackers are using this data to spearphish employees, sending e-mails purportedly from co-workers with content often too alluring or realistic to ignore. And just one breach is all they need to open the floodgates.

We have seen not only a loss of data, but also corruption of that data. We are concerned with the integrity of your source code. If hackers made subtle, undetected changes to your code, they would have a permanent window into everything you do. The same is true for those with access to hardware and software in the global supply chain.

Some in the industry have likened this to "death by a thousand cuts." We are bleeding data, intellectual property, information, and source code, bit by bit, and in some cases, terabyte by terabyte.

The solution does not rest solely with better ways to detect and block intrusion attempts. We are playing the cyber equivalent of cat and mouse, and, unfortunately, the mouse seems to be one step ahead.

We must work to find those responsible. And we must make the cost of doing business more than they are willing to bear.

We in the FBI pursue cyber threats from start to finish. We have cyber squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners.

Together, they run complex undercover operations and examine digital evidence. They share information with our law enforcement and intelligence partners, including the Secret Service, which also has strong capabilities in this area. And they teach their counterparts—both at home and abroad—how best to investigate cyber threats.

But the FBI cannot do it alone. The National Cyber Investigative Joint Task Force includes 17 law enforcement and intelligence agencies, working

side by side to identify key players and schemes. The goal is to predict and prevent what is on the horizon, and to pursue the enterprises behind these attacks.

The task force operates through Threat Focus Cells—smaller groups of agents, officers, and analysts from different agencies focused on particular threats.

For example, the Botnet Focus Cell investigates high-priority botnets. We are reverse-engineering those botnets with an eye toward disrupting them. And we are following the money wherever it leads, to find and stop the botmasters.

This week's takedown of the Mariposa botnet is one example of that collaboration. As you may know, Mariposa was an information-stealing botnet—one that infected millions of computers, from Fortune 1000 companies to major banks. And this case, like so many others, emphasized the need for global cooperation.

We have more than 60 FBI legal attaché offices around the world, sharing information and coordinating joint investigations with our host countries. And we have special agents embedded with police forces in Romania, Estonia, and the Netherlands, to name just a few.

Together, we are making progress. Last October, we worked with Egyptian authorities to dismantle a computer intrusion and money laundering scheme operating in the United States and Egypt.

With our partners in the United Kingdom, Germany, and Turkey, we dismantled Darkmarket, one of the most sophisticated online criminal syndicates—and one of the forerunners in using the Internet to buy and sell stolen financial data.

And we have worked with the Romanian National Police to arrest more than 100 Romanian nationals in the past 18 months. Four years ago, several American companies threatened to cut cyber ties with Romania because of the rampant hacking originating from that country. And yet today, Romania is one of our strongest partners.

These cases present unique hurdles in terms of jurisdiction and prosecution. We see borders as obstacles; criminals see them as opportunities.

Together, we must continue to work toward an international standard for cyber crime. And we must continue to press forward, country by country, and company by company.

In recent years, we have investigated a number of cases where financial institutions have been breached, with losses in the tens of millions.

You have likely heard about a recent global bank heist, where the hackers broke through an encrypted system to steal account numbers and PIN codes. They created more than 400 hundred fake ATM cards and recruited hundreds of mules around the world. In just 24 hours, in roughly 280 cities, they stole nearly $10 million dollars. The loss was limited only by the number of mules and the cash in the ATMs.

This was a revolutionary attack, in terms of its sophistication and its success. But our approach to finding those responsible was revolutionary as well.

First and foremost, the company came forward quickly, which was of great help to us.

We deployed a mobile FBI Cyber Action Team—a highly-trained group of agents, analysts, and experts in both computer forensics and malicious code. These teams travel the world on a moment's notice to respond to fast-moving cyber threats such as this one.

We worked closely with our counterparts here at home and overseas to investigate this attack. And we alerted our private sector partners to the potential danger so they could make the necessary patches.

Today, the top three hackers behind this attack are in custody in Eastern Europe. But the simple truth is, if this company had not come forward, we would not have been able to stop these individuals from hitting the next victim.

This is where we can be of value—not just in finding these criminals, but in making certain they cannot get to you in the first place. If we cannot prevent every attack, we must stop them from striking again and again. To do that, we need your help.

Importance of Private Sector Partnerships

Let me again emphasize the importance of private sector partnerships.

Historically, there has been a dichotomy between network security on the one hand, and the investigative process on the other. It has been the great divide between us. But it needn't be.

We in the FBI understand that you have practical concerns about reporting breaches of security. You may believe that notifying the authorities will harm your competitive position. You may have privacy concerns. Or you may think that the information flows just one way—to us.

We do not want you to feel victimized a second time by an investigation. And we know that putting on raid jackets, courting the media, and shutting down your systems is not the best way to get the job done.

We will minimize the disruption to your business. We will safeguard your privacy and your data. Where necessary, we will seek protective orders to preserve trade secrets and business confidentiality. And we will share with you what we can, as quickly as we can, about the means and methods of attack.

For example, we recently worked with our partners in the financial sector to draft an intelligence report on threat patterns in certain banking transactions. We shared that report with more than 4,000 partners. Together, we worked to limit the breadth and scope of this potential threat, and we closed the door to countless hackers.

Remember that for every investigation in the news, there are hundreds that will never make the headlines. We are behind the scenes, working to find those responsible. Disclosure is the exception, not the rule.

That said, we cannot act if we are not aware of the problem.

Maintaining a code of silence will not benefit you or your clients in the long run. It calls to mind the old joke about two hikers in the forest who run into a grizzly bear.

The first hiker says to the other, "We just need to outrun him." And the second replies, "I don't need to outrun him. I just need to outrun you."

You may well outrun one attack, but you aren't likely to avoid the second, or the third. Our safety lies in protecting not just our own interests, but our critical infrastructure as a whole.

Following World War I, France built a line of concrete fortifications and machine gun nests along its borders. It was designed to give the French army time to mobilize in the event of an attack by Germany. The secondary motivation was to entice Germany to attack Belgium as the easier target.

As we all know, the Maginot Line held strong for a brief time. However, in the long run, it did little good. The Germans invaded Belgium, flanked the line, and stormed France.

In the end, neither fortresses nor fortifications stopped Nazi Germany. Our success in defeating Germany was built on a united front. We stopped playing defense, and we pushed back, day by day. No one country, standing alone, could have ended that war.

The same is true today, in this new context. No one country, company, or agency can stop cyber crime. A "bar the windows and bolt the doors" mentality will not ensure our collective safety. Fortresses will not hold forever; walls will one day fall down. We must start at the source; we must find those responsible.

The only way to do that is by standing together. Together we can find better ways to safeguard our systems and stop those who would do us harm. For ultimately, we face the same threat. We both serve the American people. And we must continue to do everything we can, together, to minimize these attacks.

Thank you and God bless.

Robert S. Mueller was nominated by President George W. Bush and became the sixth director of the Federal Bureau of Investigation on September 4, 2001.

Mr. Mueller graduated from Princeton University in 1966 and later earned a master's degree in International Relations at New York University. After college, Mr. Mueller joined the U.S. Marine Corps where he served as an officer for three years, leading the rifle platoon of the Third Marine Division in Vietnam. He is the recipient of the Bronze Star, two Navy Commendation Medals, the Purple Heart, and the Vietnamese Cross of Gallantry.

Following his military service, Mr. Mueller earned a law degree from the University of Virginia Law School in 1973. Mr. Mueller worked as a litigator in San Francisco until 1976. He then served for 12 years in U.S. Attorney's Offices. In 1982, he became an assistant U.S. attorney. In 1989 he served as an assistant to Attorney General Richard L. Thornburgh. In 1993, Mr. Mueller became a partner at Boston's Hale and Dorr. He returned to public service in 1995 as senior litigator in the Homicide Section of the D.C. United States Attorney's Office. In 1998, Mr. Mueller was named U.S. Attorney in San Francisco and held that position until 2001.

[SPEECH]

American Health Lawyers Association Washington D.C. January 21, 2010

Individuals and health care companies that violate the fraud & abuse laws can be excluded from participation in health care programs

By Inspector General Daniel R. Levinson

This conference, "Legal Issues Affecting Academic Medical Centers and Other Related Institutions," is timely in that it focuses on a wide range of important issues currently undergoing debate that impacts researchers, teaching hospitals, academic medical centers, and the federal government. I appreciate the opportunity to speak with you today about the work of the Office of Inspector General regarding conflicts of interest.

My remarks today will focus on OIG work regarding COIs and the challenging aspect of managing, reducing, and eliminating conflicts under the current regulatory framework and system where reliance is placed primarily on individuals, researchers, and institutions. The nature and amount of information that should be reported and disclosed, and where responsibility should be placed for reviewing and verifying the information, remains a constant subject of debate within the life-sciences community and the federal government.

Background on Conflicts of Interest

First, I want to acknowledge that the vast majority of physicians and scientists are ethical and honest and committed to the welfare of their patients. AMCs play a special role in health care that is very different than other providers. First, AMCs are responsible for educating and training the next generation of physicians, nurses, and other types of health care workers. Second, AMCs serve their communities by providing uncompensated care to uninsured populations. Third, AMCs advance clinical care for the sickest patients. Fourth, AMCs advance basic science in pre-clinical research and participate in clinical trials to develop new technology. Additionally, and of great importance, AMCs are considered to be leaders in the sense that community hospitals follow the lead of AMCs.

These important roles and responsibilities bring challenges to institutions and researchers regarding potential COIs. Conflicts can arise in a variety of contexts: profit incentives to commercialize products that had successful clinical trials; questionable clinical trial results; corrupt data; purchase of drugs and devices based on commercial influence; and industry support for school, residency and continuing medical education (CME) programs. COIs can be subtle and often hard to detect. For instance, what may appear to be an appropriate arrangement between a researcher and a drug manufacturer may actually raise potential COI issues that could taint the results of a clinical trial.

The crux of the debate regarding systems for detecting and reporting potential COIs has centered on whether physicians, researchers, and institutions should be primarily responsible for reporting and managing COIs and the extent to which government regulation should place oversight and verification responsibility on federal agencies.

If COIs are undetected or are disclosed and not appropriately dealt with, the result can be serious enough to damage reputations and raise public concern about the integrity of research and

patient care. If undetected, the public may suffer numerous potential harms: people who volunteer in trials may be subjected to unnecessary risk or deprived of beneficial therapies, unsafe or ineffective drugs or devices may enter the U.S. market, patients may receive inferior therapies when safer or more effective therapies are available, and the public may waste limited Medicare and Medicaid dollars to pay for this inappropriate treatment. As a result, it is important that systems be in place to ensure that the independence and integrity of health care providers and medical researchers are maintained.

Players in the Debate Over Management of Conflicts of Interest

Congress / Media

Over the past decade the oversight of COIs has received increasing attention in Congress, the media, and oversight entities including my office. In the early 2000s, congressional committees (the House Committee on Energy and Commerce especially) held a series of hearings dealing with COIs. Most of this attention focused on NIH intramural researchers and, to a lesser degree, extramural researchers. In response to the increased attention, the NIH Director established a Blue Ribbon Panel on COI policies to look at whether or not the COI policies for intramural research were sufficient to uphold agency standards and maintain public trust in NIH and its activities, among other things. The panel found an extremely complex set of rules governing COIs at NIH. The panel made 18 recommendations with its guiding principle being that NIH employees must avoid COIs. OIG, as well, has devoted attention to COIs and ethics matters within HHS. For example, OIG issued a report on how NIH handles allegations about employee activities that might be criminal or improper, which resulted in NIH adding new guidance to the NIH policy manual.

More recently, Congress has focused increased attention on extramural COIs. For example, Senators Grassley and Kohl have conducted oversight hearings and promoted legislation on COI topics. COI hearings before the Senate Special Committee on Aging have focused on the relationships between physicians and pharmaceutical and device manufacturers. Last year, Senators Grassley, Kohl, and Klobuchar introduced S-301, the Physician Payments Sunshine Act of 2009. The bill provides for transparency in the relationship between physicians and manufacturers of drugs, devices, biologicals, or medical supplies for which payment is made under Medicare, Medicaid, or CHIP. A similar bill was introduced in the House of Representatives in July 2009. Moreover, the 2010 Omnibus Appropriations Act requires that the Secretary of HHS amend federal regulations to strengthen government and institutional oversight of financial conflicts of interest by May 1, 2010.

OIG's body of work focused on COI issues is also receiving media attention. For example, Representative Rosa DeLauro, Member of the House Appropriations subcommittee that funds CDC and NIH, reviewed a recent OIG report identifying limitations in CDC's oversight of the financial interests of Special Government Employees, and she stated that "the work of the CDC is too important to be tainted in any way." Over 300 news outlets reported on the report when it was issued.

External Organizations

Respected organizations in the academic community are also continuing to debate the appropriate roles and responsibilities of institutions and the federal government when it comes to monitoring and managing COIs. A common theme among all of the players in this debate is what information should be disclosed and who—individual, government or institution—should bear the responsibility for monitoring and managing potential COIs.

In April 2009, the Institute of Medicine published a comprehensive report on COIs with the goal to examine COIs in medicine and provide recommendations for policy and best practices. The committee that drafted the report came up with a number of conclusions that are relevant in thinking about roles and responsibilities with respect to COIs. These conclusions include that the goals of COI policies in medicine are primarily to protect the integrity of professional judgment and to preserve public trust rather than to try to remediate bias or mistrust after they occur.

The disclosure of individual and institutional financial relationships is a critical but limited first step in the process of identifying and responding to COIs. COI policies and procedures can be strengthened by engaging physicians, researchers, and medical institutions in developing conflict of interest policies and consensus standards. A range of supporting organizations—public and private—can promote the adoption and implementation of COI policies and help create a culture of accountability that sustains professional norms and public confidence in professional judgments. Research on COIs and COI policies can provide a stronger evidence base for policy design and implementation—extremely relevant to our discussion today. If medical institutions do not act voluntarily to strengthen their COI policies and procedures, the pressure for external regulations is likely to increase.

The January 2010 AHLA *Connections* article, *Be Careful What You Ask for: NIH Request for Comments on Conflicts of Interest in Research*, also discusses

the appropriate role for government and institutions in managing COIs. The article concludes that "It is critical for AMCs to recognize that institutional conflicts of interest exist, to establish an environment of vigilance against the appearance of institutional conflicts of interest, to identify such conflicts in a timely manner and to manage such conflicts to ensure the impartiality of the research."

Some institutions have taken a proactive approach with respect to COI policies and procedures in an effort to manage potential COIs and avoid or minimize additional government regulation. For instance, the owner of two research hospitals affiliated with the Harvard Medical School imposed restrictions on outside pay for two dozen senior officials who also sit on the board of pharmaceutical or biotechnology companies. And Stanford University announced plans to develop new CME programs for doctors that will be devoid of the drug industry influence that has often permeated such courses. Stanford received a $3 million grant from Pfizer, and, according to the plan, Pfizer will have no say in how the grant dollars will be spent. The goal of this new policy of transparency is to avoid activities such as pharmaceutical companies rewarding high-prescribing physicians by directing a CME provider to pay them as CME faculty, consultant, or members of a CME speakers bureau.

Department of Health & Human Services

Monitoring COIs continues to garner significant attention by HHS. In the 2009 HHS Agency Financial Report, my office continued to list ethics program oversight and enforcement, including COI issues, as a top management challenge. In response to all of the attention from Congress, the media, external organizations, and OIG work, on May 8, 2009, HHS issued an Announcement of Proposed Rulemaking to gather input from interested stakeholders regarding revisions to the federal financial COI rules issued in 1995 (42 CFR Part 50, 45 CFR Part 94, "Responsibility of Applicants for Promoting Objectivity in Research for Which Public Health Service Funding Is Sought and Responsible Prospective Contractors").

The announcement recognized that relationships between the private sector and investigators have become more complex and that the collaborations "may generate an increased potential of investigators to hold financial interests in multiple sources which, if not reported and appropriately managed, reduced, or eliminated, could introduce bias into the conduct of their research." NIH specifically requested comments regarding expansion of the scope of the regulation and disclosure of interests; definition of "significant financial interest;" identification and management of COI by institutions; assurance of institutional compliance; provision of additional information to federal officials by research institutions; and broadening of the regulations to address institutional COIs.

The American Association of Medical Colleges responded to the APRM, noting, among other recommendations, that covered investigators should be required to report to institutions all of their external financial interests directly or indirectly related to their research responsibilities, regardless of amount, and institutions should be required to submit information on managed COIs that goes beyond current regulatory requirements; but it opposes routine disclosure to NIH of full management plans themselves, unless requested by NIH.

OIG Reviews

Based on the work we have done, we believe that federal rules pertaining to COI reporting by grantee institutions place significant reliance on grantees to self-disclose and self-verify that their actions comply with federal laws. Current federal regulations require grantees to report the existence of a conflicting interest—but not the details—and to assure that the interest has been managed. However, the same regulations require grantees to make information about all indentified conflicts available to NIH, or HHS, upon request. This is why we have recommended that NIH use its current authority to request further information about reported COIs where basic information about the COI is missing and, at the same time, revise the current regulation to require grantees to report certain details to NIH about their reported COIs.

For example, we conducted two reviews of oversight and compliance with the COI regulation in 42 CFR Part 50, Subpart F, governing extramural research at NIH. In both reports, we found that COI reports received from grantees did not provide specific details about the nature or amount of the financial COIs. In our first report, we reviewed NIH's monitoring of COI reports submitted by grantees. We found that 89 percent of the reports provided to NIH lacked information about the nature of the COI and how it was addressed. Based on our findings, we conducted a second study that examined the extent to which the grantees themselves handled COIs.

For the second study, we found that 90 percent of the grantee institutions we reviewed relied solely on the researchers' discretion to determine which of their significant financial interests are related to their research and are therefore required to be reported. When researchers submitted information regarding their financial interests, we found that grantee institutions did not routinely verify it. Additionally, because nearly half of the grantee institutions we reviewed do not require researchers to provide specific

amounts of equity or compensation on their financial disclosure forms, the extent of financial interests of NIH-funded researchers is rarely known.

In both of these reports, we recommended that NIH request grantee institutions to provide it with details regarding the nature of all reported financial COIs. NIH did not agree with this recommendation. In response to our second report, NIH stated that this recommendation was not within the current scope of federal regulation but this issue was raised by NIH as a specific area for comment in the Advanced Notice of Proposed Rulemaking.

Like at NIH, vulnerabilities that we have identified in FDA's oversight of COIs provides further evidence that COIs might not be properly addressed. For instance, COI information submitted to FDA by clinical trial sponsors lacked specific details necessary to confirm that COIs were properly reported and addressed by clinical trial sponsors pursuant to various parts of 21 CFR. Currently, sponsors are required to submit financial information on clinical investigators to FDA when an application for drug approval is filed, often years after the research began. In our report on FDA's oversight of clinical investigators' financial interests, we found that 42 percent of marketing applications were missing financial information. Some of these applications were missing financial information because sponsors used the due diligence exemption to indicate that they were unable to provide financial information.

If sponsors use this exemption, regulations require them to explain why they were unable to obtain the information. However, we found that often sponsors did not explain why they were unable to obtain financial information from all clinical investigators, as required. Moreover, when sponsors did include an explanation, they most often reported that clinical investigators could not be located or failed to return the financial form.

The examples I have just mentioned highlight that although grantees and clinical trial sponsors might technically meet federal mandates, there is evidence to suggest that not all COIs are managed and resolved properly. Additionally, we have found that HHS also faces challenges in managing, reducing, and eliminating COIs. In our review of CDC's ethics program for Special Government Employees we found a systemic lack of effective oversight of COI issues.

SGEs on federal advisory committees provide expert advice to the federal government. At CDC, SGEs address important public health topics, such as breast and cervical cancer, immunization, smoking, tuberculosis, and clinical laboratory improvement. For example, in 2009, SGEs on one CDC committee made recommendations that led to the establishment of H1N1 influenza vaccination priority groups in the United States.

SGEs are temporary federal employees who are typically involved in work outside of the government in the same areas as their committees' work. Similar to regular government employees, SGEs are subject to financial disclosure and COI regulations issued by the Office of Government Ethics. However, despite this fact, we found that CDC did not require SGEs to disclose their interests completely before participating in meetings, nor did it identify or resolve all SGE potential COIs, even when adequate information identifying a COI was provided.

In 2007, 64 percent of SGEs had potential COIs that CDC did not identify and/or resolve prior to certifying their OGE confidential financial disclosure forms. For example, one SGE was a member of a committee that reviewed CDC grant applications. The SGE listed a CDC-funded grant related to committee work on his curriculum vitae, which was provided to CDC for review. Yet, CDC did not notify the SGE that he was prohibited from participating in particular matters regarding his specific employer and/or grant. These findings raise concerns regarding how COIs are handled in HHS.

Enforcement Work

Next I want to turn to our enforcement capabilities. While we would always prefer that no violation occur in the first place, by working in conjunction with our law enforcement partners at the Department of Justice and the Federal Bureau of Investigation, we have developed extensive expertise in identifying fraud, waste, and abuse and taking swift enforcement action against transgressors.

First, a few examples of recent enforcement actions related to COIs in medical education that are of special interest to AMCs. Although these cases did not involve AMCs, AMCs can learn important lessons from these examples in terms of ensuring the integrity of educational sessions they host, responsible partnerships with co-hosts or industry funding sources, and appropriate behaviors and industry relationships for medical staff serving as faculty or filling the audience for educational events.

In 2004, Pfizer paid $430 million to resolve charges relating to the off-label promotion of neurontin. Neurontin had FDA approval for use preventing seizures in epilepsy patients, but Pfizer enjoyed extensive revenue from neurontin sales for various unapproved uses, including headaches and other pain treatment. The government alleged that the company engaged in an illegal promotion scheme that corrupted the physician education process by fraudulently sponsoring medical education events on off-label neurontin uses. These educational events were purportedly indepen-

dent, but in reality they were developed and produced with extensive input from Pfizer regarding topics, speakers, content, and participants, with the ultimate goal of promoting off-label sales.

For another example, in 2007, Jazz Pharmaceuticals' subsidiary, Orphan Medical Inc. (Orphan), agreed to pay $20 million to settle charges that it had illegally marketed Xyrem, a prescription drug approved for use in narcolepsy, for off-label uses. Xyrem, also known as "GHB," has been subject to abuse as a recreational drug and is classified by the federal government as a "date rape" drug. The government alleged that the company engaged in a scheme to expand the market for Xyrem by promoting the drug to physicians for off-label indications, including weight loss and chronic pain. As part of the scheme, the government alleged that the company paid a psychiatrist tens of thousands of dollars for speaking engagements that promoted a wide range of off-label indications. Some of these speaking engagements were characterized as independent CME programs, when in fact they were promotional events approved by Orphan's marketing department.

Individuals and health care companies that violate the fraud and abuse laws can be excluded from participation in federal health care programs. This means that they cannot provide any items or services for reimbursement by the Medicare or Medicaid programs. In both of these cases, the companies entered into corporate integrity agreements, or CIAs, with OIG as a condition of avoiding exclusion and allowing their continued participation in federal health care programs. The CIAs require, among other provisions, that the companies implement written policies and procedures designed to ensure that the funding of medical educational activities, including CME, conform to federal requirements.

Industry-sponsored CME can also implicate the criminal anti-kickback statute when it is used to channel remuneration to physicians. OIG has pursued several cases where companies provided funding purportedly for "educational support," but that in reality constituted payment of kickbacks. For example, in 2006, Medtronic paid $40 million to the government and entered into a CIA to settle a range of allegations that it illegally paid spine surgeons to promote and use its spinal implant devices. The improper payments allegedly included free travel, lodging, and entertainment for physicians and their guests at lavish locations, such as Hawaii, Cancun, and Malaysia. The physicians participated in meetings the company called "discussion groups," but the sessions were actually of no or limited substance. The government alleged that the company's true purpose was simply to induce the surgeons to use Medtronic's spinal implants instead of devices sold by competitors.

Conclusion

Today, I have noted examples from our work that highlight the need for enhanced safeguards to reduce or possibly eliminate COI vulnerabilities. My office will continue to conduct work in this area. It is our hope that OIG work will continue to inform decision makers regarding specific changes that can improve the management of COI issues. Without a systematic infrastructure in place and clear roles for each stakeholder, the process for identifying and eliminating COIs will not be effective. Recommendations from OIG reports, the IOM report and journal articles, and your own professional organizations highlight the need for engaging stakeholders in a discussion about best practices for strengthening COI policies and procedures.

Daniel R. Levinson

Daniel R. Levinson has served as the inspector general for the U.S. Department of Health and Human Services since September 8, 2004. Mr. Levinson is the senior official responsible for audits, evaluations, investigations, and law enforcement efforts, relating to HHS programs and operations. He manages an independent and objective nationwide organization of over 1500 professional staff members dedicated to promoting economy, efficiency, and effectiveness in HHS programs, and addressing fraud, waste, and abuse.

Mr. Levinson has devoted a majority of his career to government service. Prior to his appointment at HHS, he served as inspector general of the U. S. General Services Administration where he oversaw the integrity of the federal civilian procurement process.

Mr. Levinson is a Phi Beta Kappa graduate of the University of Southern California, and earned a J.D. from Georgetown University where he served as notes and comments editor of The American Criminal Law Review. He is a certified fraud examiner and a member of the California, New York, and District of Columbia bars.

[SPEECH]

Federal Law Enforcement Training Center, Glynco, Ga. October 29, 2009

I am proud of the quality of Special Agents we have, here, joining the inspector general and law enforcement community.

By Inspector General Brian D. Miller

Thank you for that kind introduction. And, thank you for the fine job that you've done overseeing the completion of this class. I would also like to recognize and thank Angela Hrdlicka and the rest of the FLETC staff for their dedication, their commitment, and the hard work that they put into this course. I would also like to recognize the investigators and training staff, here, who work so hard to run this excellent program. You do a fine job, and we all owe you a debt of gratitude.

Let me also say thank you to the family members of these graduates. Thank you for your support, your sacrifice, and the crucial roles you play in these agents' lives – and will play in their careers in law enforcement.

To you graduates, Congratulations! This is quite an accomplishment. It's not easy. You have all accomplished something remarkable, something you and your families should be proud of. Without doubt, the work you will be doing as a special agent can involve risk. It can sometimes be dangerous, and it is not for everyone. This profession which you have chosen requires a special combination of courage, common sense, and sound judgment. Your instructors believe you possess all of these qualities, or you wouldn't be sitting here today. Each one of you has what it takes to succeed in this special line of work. And you are now armed with the skills and charged with the responsibility to make our country a safer place to live.

I would like especially to congratulate those of you who received awards. I am proud of the quality of Special Agents we have, here, joining the inspector general and law enforcement community. I am doubly proud that Steve Lobaugh from our office, the Office of Inspector General for GSA, won an academic prize. Congratulations, you are quite a talented group.

I am sure that you will be a credit to our federal law enforcement community. As a special agent, you represent the entire federal law enforcement community. You might be the first special agent that many people will ever meet. Sometimes you will be the only special agent, that person will ever meet. That person's image of federal law enforcement will hinge on the impression you make. Make no mistake about it, you will be scrutinized. Your conduct -- both on and off duty -- will be scrutinized by the public and others. And they will expect a lot. All of us who serve the public are held to a higher standard of conduct. The bar is set very high for all of us in public service, as it should be.

That doesn't mean, though, that you will never make mistakes. We all do that. But I keep in mind something that a former United States attorney told the office when she was sworn in. She said, "There is no problem that cannot be fixed." We all make mistakes. It's important to know what to do about them.

Just let your supervisors know and we can fix it. She also said that the sooner you let her know, the easier it is to fix. As a new AUSA, I thought that was very good advice and more than a little comforting. And that advice has helped me. I try to be quick to admit my mistakes, so we can fix them.

And I have seen this principle at work. I had a case . . . . You didn't think you would escape a war story from a former prosecutor, did you? The USA's office in West Virginia had just put away the biggest drug kingpin in its history. But soon after the kingpin began serving his life sentence, he found out that the lead agent for the task force had been having a sexual relationship with his wife all throughout the investigation and trial. The kingpin then filed motions to set aside the verdict and to throw out the case based on the misconduct of the government. The judge recused the USA's office, and DOJ asked me to lead a team of AUSAs from another district to "fix it." This was really bad misconduct, and there was more that I can tell you afterwards. But we empanelled a special grand jury, and through the incredibly hard work of Special Agent Jim Balcom from the DEA, we not only preserved the life sentences for the kingpin and his crew, but we also added charges and convictions. And I tell that war story because it shows that no matter how bad the mistake is, it can always be fixed. If those mistakes could be fixed, then surely our mistakes can also be fixed. I know I take comfort in that and you should too.

At DOJ, we had a saying, "The United States wins when justice prevails." It's good to keep that in mind. Not everyone is a bad guy, though there are many of them out there. It is just as important to exonerate the innocent as it is to make the case against the guilty. You should go only as far as the facts take you. No further, but no less! But you should never hesitate to go where the facts lead. You must aggressively pursue the bad guys. And you should never ever go beyond the facts. You may know that someone is dirty, but unless you have the facts to prove it, you have to let him or her go. You'll get them next time. And believe me, there will be a next time, especially if they think they are getting away with it. It's just not worth the insult to your integrity or to the justice system to go further than the facts. The system will work and you will get them eventually. Remember, you always have to do the right thing.

Congratulations, now, you have made it. You will have the best job in the world. Not only will you have the opportunity to analyze documents, which I like, but you will get to break down doors and arrest people --- and put your lives on the line for the rest of us! You will have incredible careers. Special agents have all the fun!

And there is no better time to be a special agent. With the Recovery Act, more federal money is going out faster than ever before in our history. Whenever Federal money goes out fast, there is fraud. You can count on it. One senator remarked, ". . . we are opening up the floodgates to fraud." Unscrupulous individuals and companies will try to take advantage of the stimulus money. And we will need you as special agents to stop them, to investigate them, and bring those criminals to justice. The American public is counting on you as special agents. We are counting on you to find fraud and prosecute those unscrupulous individuals.

This is your time. Enjoy it. Live up to the high standards that come with it. And serve the public well. Congratulations and good luck! ❧

Brian D. Miller

Brian D. Miller has served as the inspector general of the U.S. General Services Administration since July 22, 2005. Mr. Miller directs nationwide audits and investigations of federal procurement involving GSA. Mr. Miller is also a member of the Council of the Inspectors General on Integrity and Efficiency, and participated in the U.S. Department of Justice Hurricane Katrina Task Force. On October 10, 2006, Mr. Miller was named vice-chair of the National Procurement Fraud Task Force.

In 2007, Mr. Miller was recognized by Ethisphere magazine as the 12th "most influential person in business ethics" by a worldwide panel of experts. In July 2008, Mr. Miller was named among "Those Who Dared: 30 Officials Who Stood Up for Our Country," a special report of Citizens for Responsibility and Ethics in Washington, D.C., a national advocacy organization. In October 2008, Mr. Miller received the Attorney General's Distinguished Service Award.

Mr. Miller earned his law degree from the University of Texas.

[TESTIMONY]

Key Issues and Challenges Facing NASA: Views of Agency's Watchdogs

Congressional testimony before the U.S. House of Representatives, Committee on Science and Technology, Subcommittee on Space & Aeronautics (February 3, 2010)

By Inspector General Paul K. Martin

Chairwoman Giffords, Ranking Member Olson, and Members of the Subcommittee: Thank you for the opportunity to discuss the key issues and challenges facing NASA. As requested, this statement describes the Office of Inspector General's observations based on findings and recommendations from our recent oversight work, particularly our report on "NASA's Most Serious Management and Performance Challenges," which we provided to the Administrator and Congress in November 2009. Our report, which was included in the Agency's Performance and Accountability Report for fiscal year 2009, is available to the public on the OIG's Web site.

Based on our audit and investigative work, we identified five areas that we believe constitute the most serious management and performance challenges facing NASA. They are:

- Transitioning from the Space Shuttle to the Next Generation of Space Vehicles
- Managing Risk to People, Equipment, and Mission
- Financial Management
- Acquisition and Contracting Processes
- Information Technology Security

In determining whether to identify an issue as a "top management and performance challenge," we consider its significance in relation to NASA's mission; its susceptibility to fraud, waste, and abuse; whether the underlying problems are systemic; and the agency's progress in addressing the issue. Some of the challenges, such as financial management, acquisition and contracting processes, and information technology security, have confronted agency leadership for most of the past decade.

Through various initiatives, including implementing recommendations made by the OIG and other oversight bodies such as the Government Accountability Office and the Aerospace Safety Advisory Panel, NASA is working to address these and other challenges and to improve agency operations. For example, NASA has implemented a variety of corrective actions over the last several years to address long-standing weaknesses in its financial management processes and systems, reduce vulnerabilities in information technology security, and improve acquisition and contracting practices. However, NASA needs to do more to address these and other critical challenges.

The remainder of this statement provides more detail on NASA's five major management and performance challenges identified by the OIG.

Transitioning from the Space Shuttle to the Next Generation of Space Vehicles

A key challenge for NASA is maintaining the critical skills and capabilities required to fly the space shuttle safely until its retirement while transitioning to the next generation of space vehicles. In 2004, the President's Vision for U.S. Space Explo-

ration caused a substantive reorganization of NASA's strategic priorities, established a timeline for the retirement of the space shuttle, established the completion date for the International Space Station, and set the human spaceflight goals of returning to the Moon and reaching Mars. However, since that time fiscal constraints and technical challenges have hampered NASA's efforts to implement the vision effectively.

NASA continues to fund and plan for completion of the five remaining Space Shuttle flights by September 30, 2010. However, we have doubts that NASA will be able to keep to this aggressive and ambitious flight schedule. Based on calculations by the OIG, historical flight rates, the presidentially directed Review of U.S. Human Space Flight Plans Committee (the Augustine Committee), and internal NASA evaluations, NASA is not likely to meet its September 2010 timetable, and it will most likely take until the second quarter of FY 2011 to complete the last of the planned space shuttle flights. Importantly, any delay in this timetable has ramifications far beyond scheduling, given that NASA spends approximately $200 million a month to sustain the Shuttle Program.

At the request of Congress and the Administration, NASA has developed options for extending Shuttle operations and closing the gap between its planned retirement in 2010 and the planned first piloted space flight of the Constellation Program's Orion crew exploration vehicle in 2015. While technically feasible, each option involves additional shuttle flights and results in a higher cumulative safety risk associated with increased exposure to debris and potential vehicle failures. Moreover, NASA would need additional funding to avoid "borrowing" from the development of the next generation of space vehicles and other NASA programs to pay for more shuttle missions.

If the shuttle's flight schedule is extended beyond the five missions currently planned, NASA will need to re-evaluate not only funding issues, but also the sustainability of the shuttle's workforce and infrastructure, much of which has been in wind-down mode since 2009. In 2003, the Columbia Accident Investigation Board recommended that NASA complete a recertification at the material, component, system, and subsystem levels before operating the shuttle beyond 2010. In its recently released annual report, the ASAP stated that it does not support extending the shuttle program significantly beyond its current manifest. I will leave to ASAP Chairman Joseph Dyer any additional comments he cares to offer on the potential safety implications of extending the shuttle program beyond its currently scheduled manifest.

The President's FY 2011 budget, released on Monday, set out the administration's blueprint for NASA's future. Of course, this subcommittee and other committees of Congress will weigh in and help shape NASA's future direction. Amid much uncertainty, one thing is clear: NASA will need a sustained level of funding to enable successful execution of whatever future plan is ultimately adopted.

Managing Risk to People, Equipment, and Mission

NASA program and project managers face a variety of challenges associated with risks introduced by fiscal constraints, schedule demands, and changing priorities. To meet these challenges, NASA program and project managers must adhere to the fundamentals of program and project management, fully implement acquisition strategies that share risks and rewards with contractors, and effectively use earned value management systems to help agency managers identify and mitigate risks.

In the past year, the OIG dedicated considerable resources to reviewing the agency's risk management efforts at program and project levels. For example, we identified opportunities to improve the risk management processes in the Landsat Program and Orion Project. Specifically, we found that the Landsat

Data Continuity Mission was facing a cost increase and possible launch schedule delays because baseline requirements were not finalized prior to contract award.

In reviewing the Orion Project, we found that the Project Office conducted a premature life-cycle review. Instead of delaying the life-cycle review until the revised vehicle configuration was developed, the Orion project office proceeded with the review of a vehicle configuration that was under revision.

Technical issues continue to add risk to NASA projects and challenge mission success. For example:

- The Stratospheric Observatory for Infrared Astronomy Program recently resolved technological challenges with the aircraft's movable door that covers the opening to the telescope, challenges that had caused delays in flight testing.
- The Mars Science Lab suffered a major setback due to technical challenges that resulted in a missed launch opportunity in 2009, a $400 million cost increase, and a 2-year schedule delay.
- The Orbiting Carbon Observatory, a satellite important to monitoring and understanding the Earth's changing climate, suffered an undetermined technical failure on launch, resulting in the loss of the $209 million satellite and leaving a gap in NASA's ability to measure carbon dioxide in the atmosphere and its role in global warming.

Financial Management

For most of the past decade, the OIG has identified the need to improve financial management at NASA as one of the Agency's most serious management and performance challenges. In early December 2009, when I testified on this issue before this Subcommittee, I noted that while NASA has successfully implemented a variety of corrective actions over the years to address long-standing weaknesses, several challenges remain.

For example, in its most recent report the independent public accounting firm Ernst & Young disclaimed an opinion on NASA's financial statements for FY 2009, noting that it was unable to obtain sufficient evidentiary support for the amounts presented in the Agency's financial statements. This disclaimer resulted primarily because of continued weaknesses in NASA's internal controls over accounting for legacy assets – specifically, the Space Shuttle and International Space Station.

As we discussed in detail at the December hearing, E&Y identified three significant deficiencies in internal controls with one considered a material weakness. Specifically, E&Y reported a material weakness in NASA's controls for assuring that the financial statements fairly state the value of legacy property, plant, and equipment and materials. E&Y's identification of internal controls over legacy assets as a material weakness means there was a reasonable possibility that the controls were not sufficient to prevent a material misstatement in the financial statements. The other two internal control deficiencies cited by E&Y involved NASA's processes for estimating environmental liabilities and its compliance with the *Federal Financial Management Improvement Act of 1996*.

E&Y's report contained specific recommendations intended to assist NASA in remediating these weaknesses during FY 2010, to include implementing guidance allowing the use of estimates in establishing the value of legacy assets. Since the December hearing, OIG and E&Y staff have met with staff in NASA's Office of the Chief Financial Officer to discuss the Agency's efforts to address indentified weaknesses in internal controls.

While we cannot predict the success of NASA's efforts, I am hopeful that through effective implementation of E&Y's most recent recommendations and a continued focus on its ongoing monitoring and remediation efforts, the agency can correct existing weaknesses in financial management during FY 2010 to the point that E&Y can render an opinion. We will continue to work closely with NASA managers throughout the fiscal year in an attempt to achieve that goal.

Acquisition and Contracting Processes

Systemic weaknesses in NASA's acquisition and contracting processes represent another longstanding management challenge for the agency. In our November report addressing NASA's key challenges, we specifically note acquisition and contracting challenges in relation to cost estimating, acquisition processes, contract management, and ethical standards.

In recent reviews of several NASA programs, the OIG found that NASA still lacks the disciplined cost-estimating processes and financial and performance management systems needed to effectively establish priorities, quantify risks, and manage program costs. For example, in our review of the SOFIA Program, which is now 10 years behind schedule with costs more than 200 percent over initial estimates, we found that the program had not developed an independent cost estimate or implemented an earned value management plan to monitor and control program costs. Given that NASA programs and projects have historically experienced cost overruns, improvements in cost estimating using detailed, empirical data to explain program decisions could help minimize the risk of cost overruns.

GAO – which has done a lot of oversight work in this area – first identified NASA's contract management as a high-risk area in 1990, citing NASA's

undisciplined cost-estimating processes, a lack of information needed to assess contract progress, and persistent cost growth and schedule slippage in many of its major projects. In its most recent high-risk update, GAO reported improvements in NASA's processes, including its plan for addressing systemic weaknesses. I will leave it to Cristina Chaplain from GAO to provide further details on their work.

During 2009, the OIG also noted NASA's plan for addressing systemic weaknesses and improving its acquisition and contract management processes. However, our audits and investigations continue to identify weaknesses such as those we found in contracts under NASA's Small Business Innovation Research Program that bring into question the effectiveness of the program's internal controls. Given that NASA spends approximately 90 percent of its $19 billion budget on contracts and grants, it is imperative that NASA employees comply with applicable ethics laws and regulations. The scope of this ongoing challenge is underscored by the large amount of interaction between NASA employees and individuals in the private sector, both in industry and academia.

As an illustration of the challenge, NASA directives require that Standing Review Board members be independent to ensure that the boards can provide an impartial opinion of a project's potential success. Our 2009 review of membership for all Constellation Program SRBs found that 21 of the 66 non-Federal board members were employees or consultants of a NASA contractor with an interest in or contract with either the Constellation Program or one of its constituent projects.

Our review concluded that NASA's procedures for determining the independence of SRB members were inadequate. Specifically, NASA did not organize the SRBs in accordance with the Federal Advisory Committee Act requirements even though they met the definition of a FACA committee. As a result, NASA did not use the more stringent ethics review process associated with the establishment of FACA committees. Instead, NASA used a process that was lacking in both rigor and accuracy for determining the independence of SRB members. During our review, NASA suspended the activities of its Constellation Program SRBs while it addressed the FACA and conflict of interest compliance issues we disclosed.

Given the large amount of money at stake in NASA projects, the OIG's Office of Investigations has made procurement fraud and ethics a high priority. Within the past year, several OIG investigations led to criminal indictments and convictions. For example:

- A former NASA Chief of Staff was convicted on conflict of interest and false statement charges stemming from his steering of earmarked funds to a client of his private consulting company.
- A NASA SBIR contractor submitted false financial reports and improperly claimed family members on the company payroll.
- An individual working on Intergovernmental Personnel Act agreements pled guilty to conspiracy to defraud and tax evasion for payments he received from NASA and other federal agencies.
- A senior NASA scientist steered contracts to a company operated by his spouse.

These cases illustrate the types of criminal offenses the OIG pursues to help guard against waste, fraud, abuse, and misconduct. Moving forward, the OIG will continue to work with NASA ethics officials and the agency's Acquisition Integrity Program to address these issues proactively through comprehensive training while at the same time conducting vigorous investigations and enforcement.

Information Technology Security

NASA continues to face significant challenges in developing, documenting, and implementing an agency-wide program to secure its information and information technology systems. Recent breaches of NASA computer systems have resulted in the theft of sensitive data related to agency programs, which adversely affected NASA's mission and resulted in millions of dollars in losses. Over the last several years, NASA implemented a series of technical solutions that have incrementally improved the agency's overarching IT infrastructure and management practices. However, IT security remains a key management challenge. During FYs 2008 and 2009, the agency reported making progress on two key management initiatives related to IT security. First, NASA implemented the Cyber Threat Analysis Program to proactively detect and handle intrusions into NASA's cyber assets. The program includes threat analysis, identification, and reporting as well as advanced data forensics. Second, NASA initiated the Security Operations Center project to consolidate agency security operations and incident response capabilities. The SOC, scheduled to be fully operational in late FY 2010, will provide the agency with the capability to perform real-time monitoring of its computer networks and systems.

Similarly, NASA has shown progress in improving IT security as judged by our annual Federal Information Security Management Act audits. For example, in our FY 2009 FISMA audit we found that 89 percent of the 29 NASA IT systems we reviewed were certified and accredited as required. However, only 50 percent of the systems met FISMA requirements for annual contingency plan testing and only 25 percent had their security controls tested within the last year as required.

NASA is a prime target for sophisticated cyber attacks as new phishing techniques and malware programs become more advanced and destructive. In a recent incident, for example, intruders were able to steal large amounts of NASA research data, including information protected under the International Traffic in Arms Regulations. The foreign-based intruders initially compromised a single user's account but gained access to a great deal of data across a number of NASA programs because of poorly implemented access controls. This incident remains under investigation by our Computer Crimes Division, a group of highly skilled special agents and forensic technicians with advanced training in cybercrime investigations.

Our cybercrime investigations have resulted in criminal convictions or disruptions in the operations of internationally based cyber-intruders who are highly adaptive in avoiding detection. For example, a group of Romanian hackers, the so-called "White Hat Gang," penetrated and damaged a number of NASA systems integral to the Global Earth Observation System. Our agents and technicians eventually tracked one perpetrator to Arad, Romania, where local officials held him accountable in the Romanian Judicial System. Similarly, we have had investigative success against cyber-criminals from Nigeria, Portugal, Slovenia, Italy, Venezuela, and Sweden.

Finally, recommendations from our cybercrime investigations have also identified opportunities to enhance NASA's incident response training, internal coordination, and centralized command and control, leading to systemic improvements in NASA IT security. Significantly, NASA's decision to establish a Security Operations Center for centralized management of intrusion detection, response, reporting, and damage assessment was partially based on OIG recommendations supported by over four years of investigative and audit analyses.

Conclusion

We have a number of ongoing or planned reviews that address the key challenges facing NASA. For example, we are assessing critical components of NASA's efforts to transition from the space shuttle to the next generation of space vehicles. Specific areas of focus include NASA's plans for completing the remaining shuttle flights, disposing of shuttle program equipment, and estimating costs for transition and retirement activities.

In addition, we are nearing the completion of fieldwork for our reviews of the James Webb Space Telescope and the Tracking and Data Relay Satellite System. We are also conducting a review of NASA's acquisition strategy for obtaining launch services when the current contract expires in June 2010.

We continue to work with NASA to improve its financial management through both the annual audit of the agency's financial statements and our monitoring NASA's use of the $1 billion received under the American Recovery and Reinvestment Act of 2009.

In the area of acquisition and contracting, our investigative work continues to identify fraud, waste, and abuse by participants in NASA's SBIR Program. Consequently, we opened a comprehensive audit of NASA's management of the SBIR Program that will examine the sufficiency and implementation of the program's internal controls.

Finally, we are continuing to assess NASA's IT security and the agency's efforts to ensure the availability, confidentiality, and integrity of mission and mission support networks and systems.

We look forward to continuing our work with NASA leadership, this subcommittee, and other congressional committees as we seek to help the agency address its top management and performance challenges.

Paul K. Martin was confirmed by the U.S. Senate as NASA inspector general on November 20, 2009. Prior to coming to NASA, Mr. Martin served as the deputy inspector general at the Department of Justice for six years.

From 2001 to 2003, he served as counselor to the inspector general, and previously as special counsel to the inspector general from 1998 to 2001. Prior to joining DOJ's Office of the Inspector General, Mr. Martin spent 13 years at the U.S. Sentencing Commission, originally as a special assistant to the staff director when the Commission was formed in 1985, and later served as the agency's deputy staff director.

Mr. Martin began his career as a reporter with the Greenville News in Greenville, S.C. He holds a bachelor's degree in journalism from Pennsylvania State University and a Juris Doctorate from Georgetown University Law Center.

[TESTIMONY]

Afghanistan Reconstruction

Congressional testimony before Commission on Wartime Contracting (February 22, 2010)

By Inspector General Arnold Fields

Chairman Thibault, Chairman Shays, and members of the Commission:

Thank you for inviting me this morning to discuss SIGAR's work and the issues we believe must be addressed to improve the effectiveness of the expanding reconstruction effort in Afghanistan.

Since 2002, Congress has appropriated more than $51 billion to rebuild Afghanistan. This figure will grow in FY 2011 and, in all likelihood, surpass the $53 billion that has been provided for Iraq's reconstruction. While this amount may appear small compared with the trillion dollars the United States has spent on the military campaigns in both Iraq and Afghanistan, it is by any other measure a lot of money. And, the success of the U.S. strategy in Afghanistan depends to a large degree on the effective use of these funds to build the Afghan security forces, improve governance, and lay the foundation for sustained economic development. Ultimately, the future of Afghanistan will be determined by the people of Afghanistan and their confidence in their government.

I am often asked why we need a Special Inspector General for Afghanistan Reconstruction. After all, each implementing agency has its own inspector general and we also have the Government Accountability Office that reports to Congress. What does a special inspector general bring to an oversight table that some might consider already crowded?

My answer is this: In Afghanistan, SIGAR is bringing focused oversight to reconstruction activities that are funded through and implemented by multiple agencies. We not only look at individual projects and contracts, but at how these projects and contracts fit into larger programs and work together to support U.S. strategic goals in a country deemed critical to U.S. national security. We look at how U.S. agencies coordinate with each other and at how these agencies have integrated U.S.-funded programs with those of the international donor community to realize reconstruction objectives. At the end of every quarter, we provide a report to Congress that summarizes current and historical data on reconstruction activities: no other agency has this broad legal mandate.

SIGAR—through its audits and investigations—seeks to improve the effectiveness of U.S. programs and deter fraud, waste, and abuse by fostering a culture of accountability that permeates every aspect of the reconstruction effort in Afghanistan. What do we mean when we talk about accountability? Obviously, the first thing is knowing where the money is going. However, my auditors are looking at much more than whether agencies and their implementing partners are keeping good records of expenditures. We want to know if they have the controls in place to mitigate against fraud. Is the money going for activities to achieve objectives that support the larger U.S. goals? Are there metrics in place to measure progress? Are projects and activities coordinated with others to prevent duplication of effort? Is our money being used for activities that will have a lasting effect? Does the Afghan government have the ability to operate and maintain infrastructure? What are we doing to help the Afghan government build capacity to sustain education, health, and rule of law programs so that our money is not wasted?

We believe that everyone involved in reconstruction—from the U.S. government agencies and contractors to

the Afghan government, which is the beneficiary of our assistance—has a responsibility to provide good stewardship of public funds. SIGAR's work to date has shown that all these groups need to do much more to be accountable for the reconstruction money the United States is spending in Afghanistan.

Implementing Agencies

The primary obligation for oversight must, in my view, rest with the agencies administering funds. The Department of Defense, the Department of State, and USAID have been allocated the majority of reconstruction funds for Afghanistan, but the Departments of the Treasury, Justice, Homeland Security, and Agriculture also have significant roles in helping to rebuild that country. Each of these agencies is responsible for spending taxpayer dollars carefully and wisely.

These agencies fund a number of activities not only through contracts with the private sector, but also through cooperative agreements and grants with entities such as non-profit organizations and offices of the United Nations. It might surprise some observers to learn that less than half (2.5 billion) of the $5.4 billion obligated by USAID for reconstruction in Afghanistan between FY 2002 and FY 2009 went to private sector contractors. USAID spent nearly $3 billion through cooperative agreements ($1.67 billion) and grants ($1.29 billion). Contracting is important, but in the context of reconstruction in Afghanistan, it is also essential to assess other mechanisms, such as these cooperative agreements and grants, that are being used to fund reconstruction activities.

The ability of an agency to oversee its programs depends to an extent on its financial management system. At the end of November last year, President Obama issued an executive order to intensify efforts to eliminate payment error, waste, fraud, and abuse in the major programs administered by the federal government. This directive targets high dollar federal programs and requires federal agencies to develop methodologies to identify and measure improper payments associated with these priority programs. This is a good step toward making agencies more accountable, but it does not address reconstruction funding.

SIGAR has begun a forensic analysis, which will use data mining and anomaly detection techniques to identify potential fraud and waste in the billions of dollars spent for Afghanistan reconstruction. This analysis is intended to identify targets for focused audits and criminal investigations. However, SIGAR believes that each implementing agency should have the financial management systems in place to analyze its own data and identify payment anomalies on a regular basis to detect fraud and waste. This is not the case today, but it should be an integral part of each agency's oversight of its own programs.

In Afghanistan, several agencies are often involved in designing and implementing projects that are part of larger programs. In Afghanistan, unlike Iraq, the international community is also making significant contributions to some programs. This is true for the nearly $27 billion the United States has allocated to develop the Afghan National Security Forces. The Departments of Defense and State as well as the international community, through our NATO partners, have contributed human and financial resources to this effort. Multiple U.S. agencies and international partners are also involved in many other activities, including our justice and counternarcotics programs and for the recently announced initiative to strengthen the agricultural sector in Afghanistan. Successful reconstruction in Afghanistan requires significant inter-agency cooperation and coordination with the international community.

SIGAR is conducting a variety of audits to assess 1) the ability of individual agencies to manage and oversee their programs, and 2) the degree to which agencies coordinate programs with each other and with the international community. Eight months ago SIGAR issued an audit that found that the Combined Security Transition Command-Afghanistan, which is responsible for training the Afghan National Security Forces, did not have the contracting officials it needed to properly monitor a $400 million contract. U.S. commanders in Afghanistan welcomed this audit and used it to make their case for recruiting more contracting officers. Nevertheless, during my visit to Afghanistan last month U.S. commanders told me that they still do not have the contracting officers needed to oversee the large training contracts. The Defense Department has not provided CSTC-A with the full measure it needs to implement and oversee our most critical programs.

Experience in Iraq and elsewhere has shown that taxpayer dollars may be wasted because projects are measured by outputs rather than outcomes. This is because it is easier to establish output metrics than outcome metrics. For example, let us say we have a training program for 20 judges or prosecutors or teachers. The question we must ask ourselves is not how many judges, prosecutors and teachers we have trained, but rather what is the consequence of this training. What do these judges, prosecutors, and teachers do as a result of the training? Implementing agencies need to be more focused on outcomes.

The United States has committed more than half of all U.S. reconstruction dollars in Afghanistan to developing the Afghan National Security Forces. The current goal of the United States, the international community, and the Afghan government is to increase the Afghan National Army to 134,000 and the Afghan National Police to 109,000 by September this year. A rating system is

used to measure the capabilities of these forces. We are conducting an audit to evaluate the reliability of this rating system as a true measure of the capabilities of the security forces. Numbers may be important. The real question is not how many troops we have trained, but rather whether our programs are developing national security forces capable of protecting the Afghan people and defending the Afghan state so that U.S. forces can withdraw.

We believe that it is necessary to conduct a broad spectrum of audits. Our auditors are therefore conducting reviews of individual contracts, agency oversight, and programs to assess whether the reconstruction program is helping the U.S. achieve its strategic goals in Afghanistan. Last month, SIGAR issued two audits in the energy sector that demonstrate our approach to oversight. One assessed a single USAID project—the $300 million Kabul Power Plant—which has experienced serious delays and cost overruns. The other audit reviewed U.S. and international projects across the energy sector. Taken together, these two audits identified systemic problems at both the project and program level that need to be addressed if the United States, its international partners, and the Afghan government are going to achieve their objective of expanding Afghan citizens' access to electricity. Our reports highlighted the absence of an updated national energy plan for Afghanistan, the lack of common electrical standards for projects, inadequate coordination between the international community and the Afghan government, poor contract management, and questions about sustainability.

Contracts and Contractors

Since I am here with the Wartime Contracting Commission, let me spend a couple of minutes talking specifically about contractors in Afghanistan and their changing role as the U.S. begins to implement its new development strategy in the country.

The United States depends on private sector contractors to perform a wide variety of reconstruction activities. These include everything from billion-dollar infrastructure contracts to multi-million dollar contracts to train the Afghan National Army and the Afghan National Police. Implementing agencies have contracted with the private sector to build everything from power plants and roads to schools, clinics, courthouses, and prisons. Contractors are developing alternative agriculture projects, running a wide variety of training and capacity-building programs, and providing security for reconstruction activities.

These contractors must be held accountable. They need to have systems in place to ensure that they complete projects in compliance with their statements of work on time and within budgets. The contractors, no less than implementing agencies, must properly track expenditures and provide quality assurance. The onus is on the prime contractors to monitor subcontractors to ensure they deliver a quality product.

SIGAR is conducting a number of focused contract audits. We have ongoing reviews of construction contracts to build army and police facilities in three different provinces. We are also assessing the U.S. Army Corps of Engineers' contract with a private security firm to determine if the Corps is receiving the services it requires at a reasonable cost. This focused contract audit is related to a review we are conducting to identify the number and volume of contracts in place to provide security services in Afghanistan.

While U.S. agencies will continue to rely on private contractors to implement many of their reconstruction programs in Afghanistan, the new U.S. strategy in Afghanistan and elsewhere is to work in greater partnership with host governments. At the latest international conference on Afghanistan, which was held in London last month, the United States and other donors pledged to increase the proportion of development aid delivered through the Afghan government to 50 percent in the next two years. This support depends on the Afghan government making progress in several areas, including strengthening its public financial management systems, improving budget execution, and reducing corruption.

Afghan Government Capacity

We believe that the Afghan government should be much more involved in every aspect of reconstruction. However, Afghan institutions must have the capacity and desire to manage the funds and protect them from waste, fraud, and abuse, and other forms of corruption.

Everyone—the donors, international organizations, and the Afghan government—is justifiably concerned about widespread corruption in Afghanistan. No one is more upset than the Afghan people themselves. A recent survey of 12 provinces by the United Nations Office on Drugs and Crime found that the average Afghan is more concerned about corruption (59 percent) than insecurity (54 percent) or unemployment (52 percent). Half of the Afghans surveyed said they had to pay at least one kickback to a public official during the preceding 12 months. The average amount was $160—this in a country where the per capita GDP is only $425 per year.

The UN estimates that Afghans paid $2.5 billion in bribes to their government officials and members of the police force in 2009. That is about 25 percent of Afghanistan's GDP and almost as much as is generated by the illicit drug trade. As the UN pointed out, the shocking reality is that drugs and bribes are the largest income generators in Afghanistan, amounting to about half the

country's recorded GDP.

Bribery robs the poor, causes misallocation of resources, and destroys trust in the government. It is understandably hard for people who earn less than $2 a day, but must bribe officials to obtain basic services, to have confidence in their government. Because corruption corrodes the government's legitimacy and undermines international development efforts, strengthening the Afghan government's capability to fight corruption must be an integral part of the U.S. reconstruction effort.

It is my firm belief that Afghan government institutions, no less than U.S. agencies and contractors, must be held accountable for all monies at their disposal. It is for this reason that SIGAR launched an anti-corruption initiative last year to 1) assess what the United States and other donor countries are doing to build the capacity of Afghan institutions to deter corruption and strengthen the rule of law and 2) determine the extent to which various national and local institutions have systems in place to account properly for donor funds.

In December SIGAR issued an audit on the High Office of Oversight, Afghanistan's principal organization responsible for overseeing and combating corruption. We found that this key office needs significantly more authority, independence, and donor support to become an effective anti-corruption institution. President Karzai, who has vowed to tackle corruption across his government, told the international conference in London last month that he would, through a presidential decree, empower the High Office of Oversight to investigate and sanction corrupt officials, and lead the fight against corruption. If President Karzai does as he has promised, he will be implementing one of SIGAR's key recommendations.

SIGAR has two ongoing audits as part of our anti-corruption initiative. The first is reviewing U.S. and other donor efforts to strengthen the capabilities of Afghanistan's Control and Audit Office. The second is assessing the Afghan government's ability to account for U.S. government payments of salaries to Afghan government officials and advisors. Our anti-corruption initiative will help identify institutions we can work with as partners; it will also help identify areas where we can use our reconstruction dollars to improve accountability. We are expanding this program and plan to have more than 20 auditors working at the national and provincial levels by the end of the year.

When you talk to U.S. and international officials about Afghanistan, they say that the future depends on one thing: improved governance. And that in turn depends on reducing corruption. Neither our military might nor all the reconstruction dollars in the world—no matter how well projects are designed and executed—can produce a secure and stable Afghanistan if the people of that country do not believe in their government. This is why we must strive to work with our Afghan partners to transform a culture of corruption into a culture of accountability. This must be at the very heart of our reconstruction effort and if we fail, we will have surely wasted scores of billions of our taxpayers' dollars.

My personal goal and the goal of my entire staff is to see our implementing agencies and the governing institutions in Afghanistan improve their capacity to conduct the oversight needed to be accountable to U.S. and Afghan citizens. Accountability is at the core of good governance.

I appreciate the opportunity to share with you our observations on the reconstruction effort in Afghanistan and look forward to continuing to work with this commission as you pursue your important mission.

Arnold Fields (Major General Ret.) is the inspector general of the Special Inspector General for Afghanistan Reconstruction, a position to which he was appointed by the president of the United States on June 12, 2008. General Fields was sworn into office on July 22, 2008 by the Deputy Secretary of Defense and reports directly to the Secretary of State and the Secretary of Defense. General Field's mandate requires that he report directly to Congress on audit investigations and other matters relating to amounts appropriated or otherwise made available for the reconstruction of Afghanistan. Previously, General Fields served as the deputy director of the Africa Center for Strategic Studies, Department of Defense. Prior to that position, he served as a member of the U.S. Department of State assigned to the U.S. Embassy in Iraq where he performed duties as the chief of staff of the Iraq Reconstruction and Management Office.

General Fields retired from the U.S. Marine Corps in January 2004, after over 34 years of active military service. He holds a Bachelor of Science degree in agriculture from South Carolina State University and a Master of Arts degree in human resources management from Pepperdine University.

[TESTIMONY]

Challenges with Afghan National Security Forces Training Contracts

Congressional testimony before Commission on Wartime Contracting (December 18, 2009)

By Kenneth P. Moorefield

Chairman Thibault, Chairman Shays and distinguished members of the Commission. Good morning and thank you for the opportunity to appear before you on behalf of the Department of Defense Office of Inspector General. Today, in response to your invitation, I would like to share with you our experiences and views regarding the challenges and risks associated with contingency contracting in support of the U.S. commitment to train and mentor the Afghan National Security Forces.

Background

The assistance provided by contractors in support of the development of the ANSF has proven to be indispensable, as it did in the growth of the security forces of Iraq. Contract personnel have played many key roles augmenting DoD, and specifically the Combined Security Transition Command-Afghanistan, in the capacity building of the Ministry of Defense and Ministry of Interior, especially in the area of systems development.

Embedded in the ANSF, U.S. contractors work as mentors and subject matter experts at the corps level and below. They manage police basic training centers, and serve as part of police mentoring teams embedded with provincial and district national police.

Contracted companies are also building training and basing facilities across the country essential to ANSF growth.

In addition to contributing specialized skills, many contract personnel have been in Afghanistan far longer than their military or civilian counterparts. Their continued presence has provided a significant degree of continuity and stability to progress made in establishing Afghan National Army and Afghan National Police capability to operate independently and assume security responsibility.

Contracting Issues and Challenges

Construction

The train, mentor, and equip mission to develop an effective ANSF poses the same uniquely complex problems to our contractors as it does to U.S. government personnel. Outside of Kabul, Kandahar, Herat, and Masar-e-Sharif, for example, there is still relatively little infrastructure to support widely disbursed ANA and ANP operations. Buildings, if they exist at all, are often little more than mud-huts. The transportation system is marginal, and severe weather conditions make remote mountain bases virtually inaccessible part of the year. Roads still have to be built to be able to supply many new military or police bases or outposts, and much of the construction material, to include cement, must be transported overland into the country.

Illiteracy in excess of 70 percent, extensive poverty and related endemic corruption are an everyday reality. Any piece of land suitable for construction of an ANSF facility first has to be de-mined and conflicting claims of ownership resolved among sometimes numerous competing individuals and families claiming legitimate title. Addressing these claims

can sometimes delay projects for over a year.

Moreover, in recent years, increasing numbers of improvised explosive device attacks by Taliban insurgents on the main roads have disrupted construction convoys, and Taliban use of extortion, kidnapping, and murder at construction sites has discouraged contractors from operating in any area not sustainably secured.

Efforts via the "Afghan First" program to hire Afghan companies and Afghan personnel to construct needed roads and facilities remain a priority contracting commitment, but implementation has proven problematic. Realistically, there are few Afghan companies with the requisite experience to effectively bid on and undertake projects. In some instances, those Afghan companies that were hired proved unable to meet contractual timing and quality requirements. As a consequence, the Combined Security Transition Command-Afghanistan and the U.S. Army Corps of Engineers' Afghan Engineer District have often had to rely on U.S. or third-country contractors in order to move forward with the construction necessary to support development of the ANSF.

As a result, necessary construction projects to support ANSF expansion often has been delayed and, in some cases, stopped altogether in areas found to be insufficiently secure.

Contract Oversight Issues

DoD IG has reported in previous congressional testimony this year that the size and skill of the DoD acquisition workforce did not keep pace with the growth of its contract oversight responsibilities in the Southwest Asia contingency operations. A relatively small number of inexperienced civilian and military contract administrators and support personnel were assigned far-reaching responsibilities for an unreasonably large number of contracts. Our OIG report issued this September on "U.S. and Coalition Plans to Train, Equip, and Field the Afghan National Security Forces" validated this concern, finding that the lack of appropriate oversight support for CSTC-A contracts had resulted in an ongoing failure to ensure that contractors selected had the required expertise to meet contract performance standards.

DoD contracting challenges and issues in Afghanistan have been exacerbated by a chronic shortage of qualified personnel. Besides not having sufficient contracting officers and contracting officer representatives, their rapid turnover caused by short three to six-month tours contributed to a deficiency in contracting oversight continuity and performance. Additionally, the Joint Contracting Command – Iraq/Afghanistan expressed concerns to our assessment team last spring over the adequacy of basic contracting officer's representative training, as well as the limited experience of those being assigned.

Some progress has been made in strengthening DoD contracting personnel capability in Afghanistan. In response to concerns expressed in the September DoD IG report on the ANSF Train and Equip Mission, the Defense Contract Management Agency reported that they had realigned resources in-theater, significantly increasing personnel assigned to the country. The Afghan Engineering District also has reported that the U.S. Army Corps of Engineers is addressing its personnel resource deficiencies identified, increasing the number of staff authorized and assigned to Afghanistan to provide additional quality assurance oversight of their construction project responsibilities. We are advised the drawdown in Iraq will free up additional contract oversight personnel, .

Transfer of Afghan Police Training From State to the Department of Defense

One issue in which the commission has expressed specific interest is that of the pending transfer of responsibility for the primary police training program in Iraq. Since 2005, the State Department has managed ANP basic training through its contract with DynCorp. Funding for that contract was provided to the State

Department by DoD. Earlier this year, the Senate Appropriations Committee requested an audit of the administration and expenditure of DoD-appropriated funding supporting the contract. The DoD-DOS team formed for this purpose anticipates issuing its final report by the first of the coming year.[1]

The DOS has already agreed to transfer responsibility for the DynCorp police training contract to DoD when it expires in January 2010. We understand that this decision was based on a mutual recognition by the two departments that the lack of a single, unified chain of command for police training had hindered flexible execution of the training program.[2]

To facilitate contract responsibility transfer from DOS to DoD, at the recommendation of the joint audit team, a transfer oversight working group was formed in August to manage such transition issues as government property, resource management and logistics, and future contracting.

As with all contracts undertaken to train and develop the ANSF, it will be incumbent upon DoD to ensure that Combined Security Transition Command-Afghanistan has a cadre of contracting officer representatives and contracting officer technical representatives in place able to provide appropriate oversight of the next police training contract's execution, particularly given its important role in any future ANP expansion.

I thank the Committee for this opportunity to present a DoD IG perspective on contracting roles and challenges in Afghanistan as they impact the capacity development of ANSF. The importance of successfully accomplishing that mission was underscored in the president's recent policy strategy determination on the way ahead in Afghanistan. And, we at DoD IG are very mindful of the contingency contracting oversight responsibilities this will entail.

I would welcome any questions you may have.

1 Report was issued on February 9, 2010 (D-2010-042)

2 The transfer of the DynCorp contract from DOS to DoD has been delayed due to the problems in the contracting process.

Kenneth P. Moorefield is the deputy inspector general for Special Plans and Operations, Department of Defense Office of Inspector General. He leads an office dedicated to facilitating informed decision-making by senior leaders of the DoD and Congress by providing assessments of priority national security challenges.

Prior to joining the Office of Inspector General, Ambassador Moorefield served as a senior State Department representative on the Iraq/Afghanistan Transition Planning Group.

Having attained the Foreign Service rank of Career Minister, he was sworn in as Ambassador to the Republic of Gabon and the Democratic Republic of Sao Tome and Principe on April 2, 2002. Prior to this appointment, Ambassador Moorefield had over 30 years of experience in the U.S. military, foreign, and civil services.

As an Army infantry officer, he served two tours in Vietnam. Among his military and civilian awards, and decorations are the Silver Star, Purple Heart, the Vietnamese Cross of Gallantry, and Superior and Presidential Honor Awards.

Ambassador Moorefield graduated from the U.S. Military Academy at West Point and took advanced international studies at Georgetown University School of Foreign Service.

Invitation to Contribute Articles to the Journal of Public Inquiry

The Journal of Public Inquiry is a publication of the Inspectors General of the United States. We solicit articles from professionals and scholars on topics important to the Inspector General community.

Articles should be approximately four to six pages (2,000-3,500 words), single-spaced, and e-mailed to: JournalofPublicInquiry@dodig.mil

To join the mailing list, please provide your name and address by e-mail to: JournalofPublicInquiry@dodig.mil

Disclaimer: The opinions expressed in the Journal of Public Inquiry are those of the authors. They do not represent the opinions or policies of any department or agency of the U.S. government.

Journal
of Public Inquiry

Inspector General Act of 1978, as amended Title 5, U.S. Code, Appendix

2. Purpose and establishment of Offices of Inspector General; departments and agencies involved

In order to create independent and objective units--

(1) to conduct and supervise audits and investigations relating to the programs and operations of the establishments listed in section 11(2);

(2) to provide leadership and coordination and recommend policies for activities designed (A) to promote economy, efficiency, and effectiveness in the administration of, and (B) to prevent and detect fraud and abuse in, such programs and operations; and

(3) to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action;